POSITIVE TECHNOLOGIES

MaxPatrol VM

Система управления уязвимостями нового поколения

Сергей Сухоруков

ведущий эксперт центра компетенции

ptsecurity.com

Эволюция средств управления уязвимостями

ptsecurity.com

От проверки портов до VM

GEN 1

СЕТЕВЫЕ СКАНЕРЫ УЯЗВИМОСТЕЙ

Сканирование в режиме черного ящика, определение открытых портов

GEN 2

СИСТЕМЫ АНАЛИЗА ЗАЩИЩЕННОСТИ

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

NEXT GEN

СИСТЕМЫ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ НОВОГО ПОКОЛЕНИЯ

Управление активами, построение процесса приоритизации и контроля устранения уязвимостей

Результаты
опроса ИБ-специалистов

В СРЕДНЕМ
>6 МЕСЯЦЕВ
не устраняются критично опасные уязвимости на важных активах

9%
СПЕЦИАЛИСТОВ
отправляют отчет об уязвимостях в IT-отдел без фильтрации

11%
СПЕЦИАЛИСТОВ
вынуждены обосновывать IT необходимость устранения каждой уязвимости

БОЛЬШАЯ ЧАСТЬ ВРЕМЕНИ
уходит на то, чтобы:
- проанализировать результаты сканирования
- убедить IT-отдел в необходимости поставить патчи

11%
КОМПАНИЙ
вообще не проверяют, устранил ли IT-отдел уязвимости

57%
СПЕЦИАЛИСТОВ
в приоритизации уязвимостей доверяют оценке по CVSS

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

Что мешает
сканировать IT-инфраструктуру?

Проблема №1: **Нет полноты покрытия IT-инфраструктуры**

- Сложно учитывать постоянные изменения в АС
- Сложно сопоставить результаты сканирования узлов сети
- Нет классификации активов по важности
- ИБ-шник не в курсе активов, которые есть в инфраструктуре
- IT-инфраструктура большая, а окна для сканирования узкие

Что мешает
реагировать на уязвимости?

Проблема №2: **Уязвимостей слишком много**

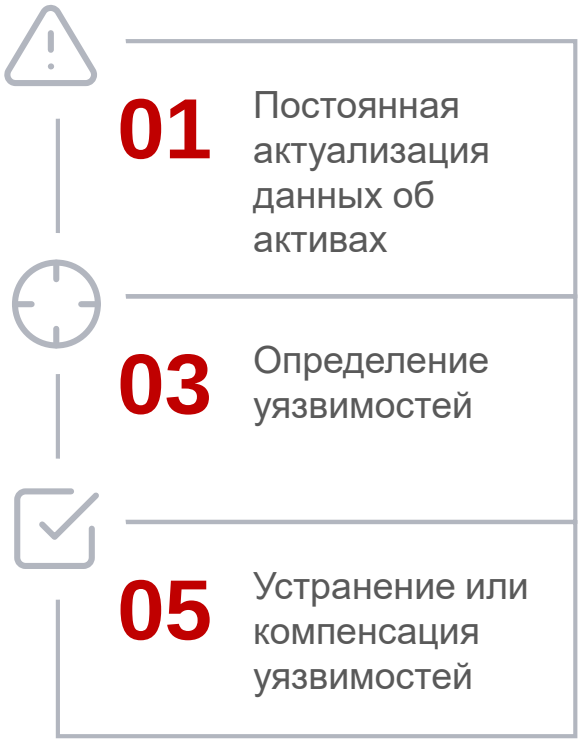
- Уязвимостей много, нет возможности все разобрать вручную
- Нужно помнить о принятых компенсационных мерах
- Нет понимания, какие уязвимости реально опасны именно для данной инфраструктуры, как грамотно приоритизировать задачи
- Нужно тратить время на чтение внешних ресурсов, чтобы не пропустить появление новых особо опасных уязвимостей

Что мешает
устранять уязвимости?

Проблема №3: **Нужно договариваться с IT-отделом**

- Для устранения уязвимостей приходится каждый раз договариваться с IT-отделом
- IT-шников много, а специалист по VM один
- Как выстроить правильные отношения с IT?
- Как часто IT действительно патчит уязвимости?
- Как контролировать устранение уязвимостей?

Управление уязвимостями



01 Постоянная актуализация данных об активах

03 Определение уязвимостей

05 Устранение или компенсация уязвимостей

02 Классификация и оценка активов

04 Сортировка и приоритизация уязвимостей

06 Проверка устранения уязвимостей

VM

AM **Asset management**
Управление активами

VA **Vulnerability assessment**
Определение уязвимостей

VR **Vulnerability remediation**
Устранение уязвимостей

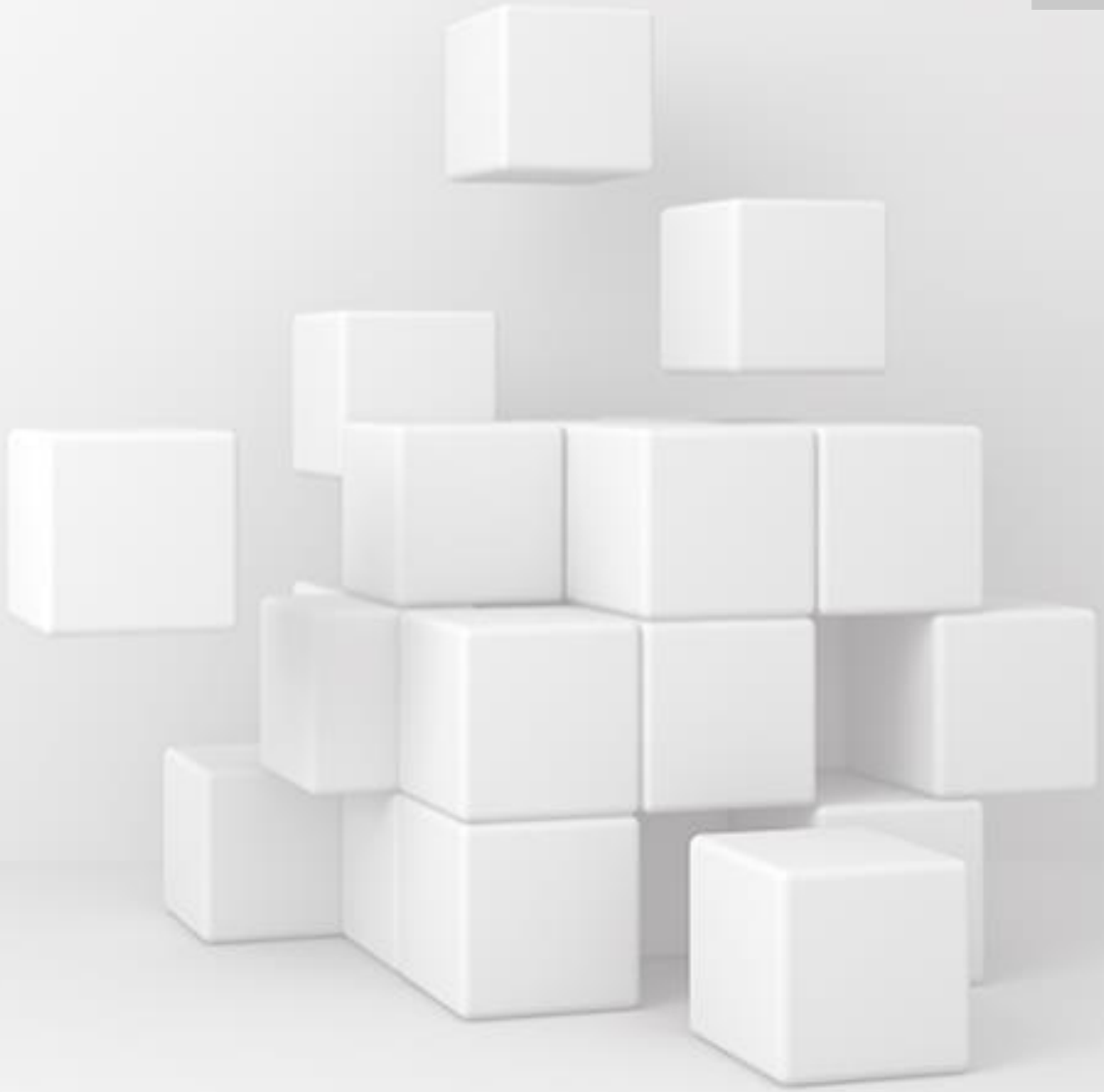
Манифест VM

процессы, уязвимости, люди

ptsecurity.com

Как не надо строить VM

- Ставим патч только там, где нашли уязвимость.
- Ставим только те патчи, где 100% подтвердилась уязвимость.
- Отправляем 100 000 найденных уязвимостей в виде тикетов в сервис деск.
- Обрабатываем только ограниченную часть уязвимостей, не обращая внимания на остальные.



Проблемы при выстраивании VM

- Нет понимания, что есть в сети.
  Как отследить все узлы?
- Уязвимостей много.
  Слишком много!
- В сети постоянно появляются и исчезают
  новые узлы. Как успевать что-то делать?
- IT-шников много, а специалист
  по VM один. Как выстоять?

Проблемы при выстраивании VM

- Нет понимания, что есть в сети. Как отследить все узлы?
- Уязвимостей много. Слишком много!
- В сети постоянно появляются и исчезают новые узлы. Как успевать что-то делать?
- IT-шников много, а специалист по VM один. Как выстоять?

Что мы хотим от VM

- Чтобы процесс охватывал все системы и сети
- Системно отслеживать повышение уровня защищенности компании
- Информирование о самых приоритетных и критичных задачах
- Возможность справиться с процессом даже одному ИБ-специалисту

Как мы это видим

Процесс VM

Плановая обработка уязвимостей

- Процесс накрывает всю инфраструктуру
- ИБ следит за качеством покрытия
- В IT принят процесс Patch Management — не зависящий от ИБ
- ИБ следит не за появлением\закрытием уязви-мостей, а за соблюдением договоренностей IT

Особо опасные уязвимости

- Срез в режиме реального времени
- Отлов особо опасных. ИБ формирует списки активов, ОС и ПО для реагирования
- По каждой уязвимости ИБ и IT отдельно договариваются о сроках устранения

Общий процесс VM

Обработка Особо Опасных

Как не надо делать

Когда в мире появилась страшная уязвимость, не надо бежать и пытаться сканировать.

Нет времени подтверждать или опровергать её наличие на критических узлах и сегментах.

Любое сканирование - это сложно согласуемый процесс, который в любом случае потратит драгоценное время.

Необходимо сделать вывод о наличии уязвимости на основе собранной ранее информации о конфигурации и сразу же переходить к этапу PM или компенсирующих мер.

Обработка Особо Опасных

MaxPatrol VM

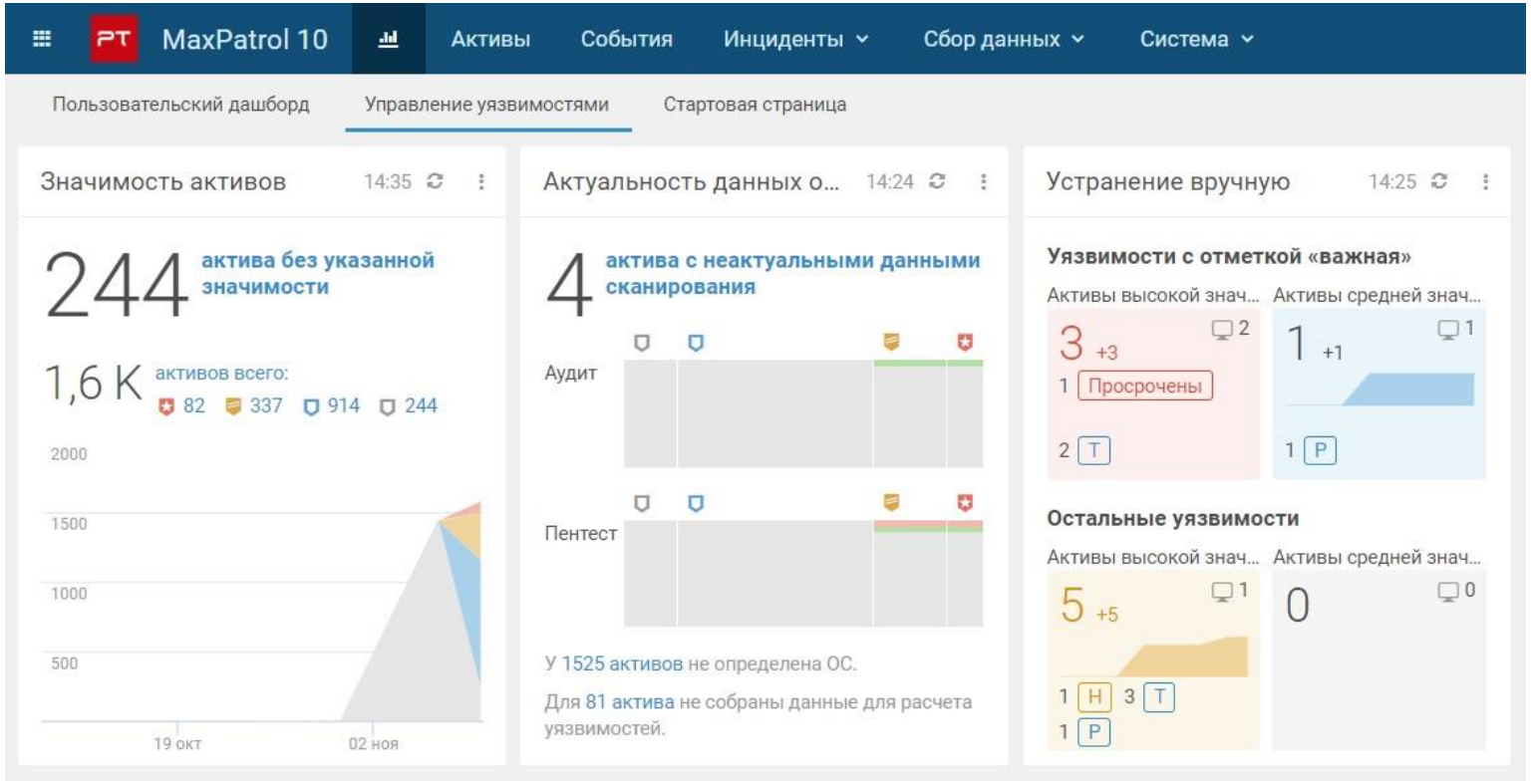
поможет выстроить процесс управления уязвимостями

ptsecurity.com

Новое решение

MAXPATROL VM

Система нового поколения для управления уязвимостями



MaxPatrol VM отражает новый подход к безопасности

Решение, которое поможет построить **полноценный процесс** управления уязвимостями и сделать реализацию конкретных рисков компании слишком **дорогой и сложной** для злоумышленника.

MaxPatrol VM

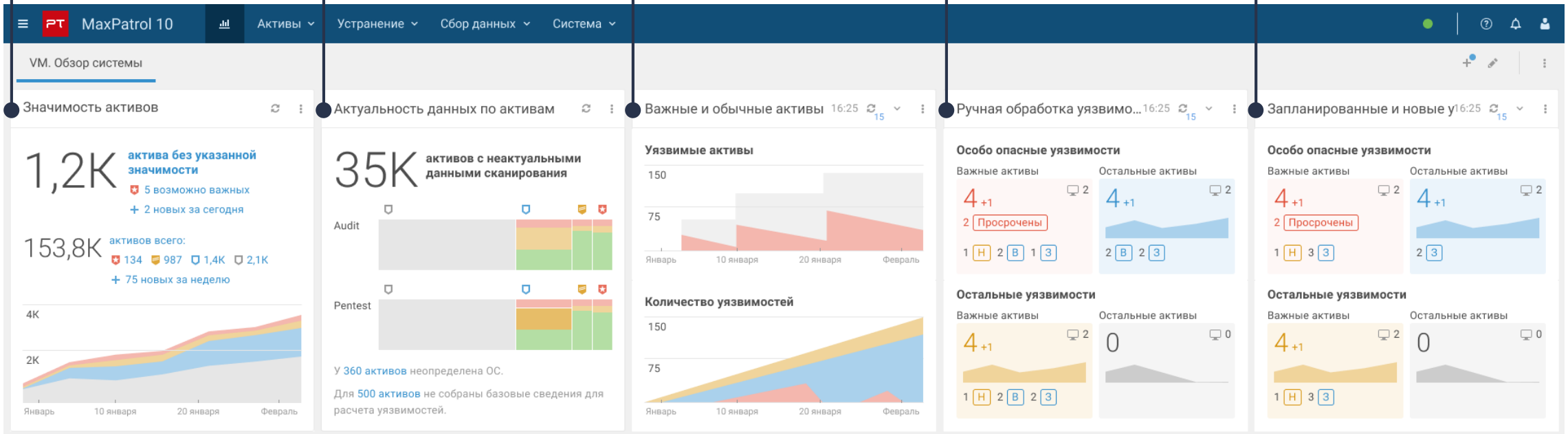
Нашли все активы в сети. Приоритизируй, чтобы знать что важно

Получи свежую инфу про активы и их уязвимости. Задай политики сканирования

Контролируй, что происходит на важных активах. Отслеживай новые активы

Обычные уязвимости фиксит IT в рамках политик и SLA. Безопасник должен смотреть только за особо опасными

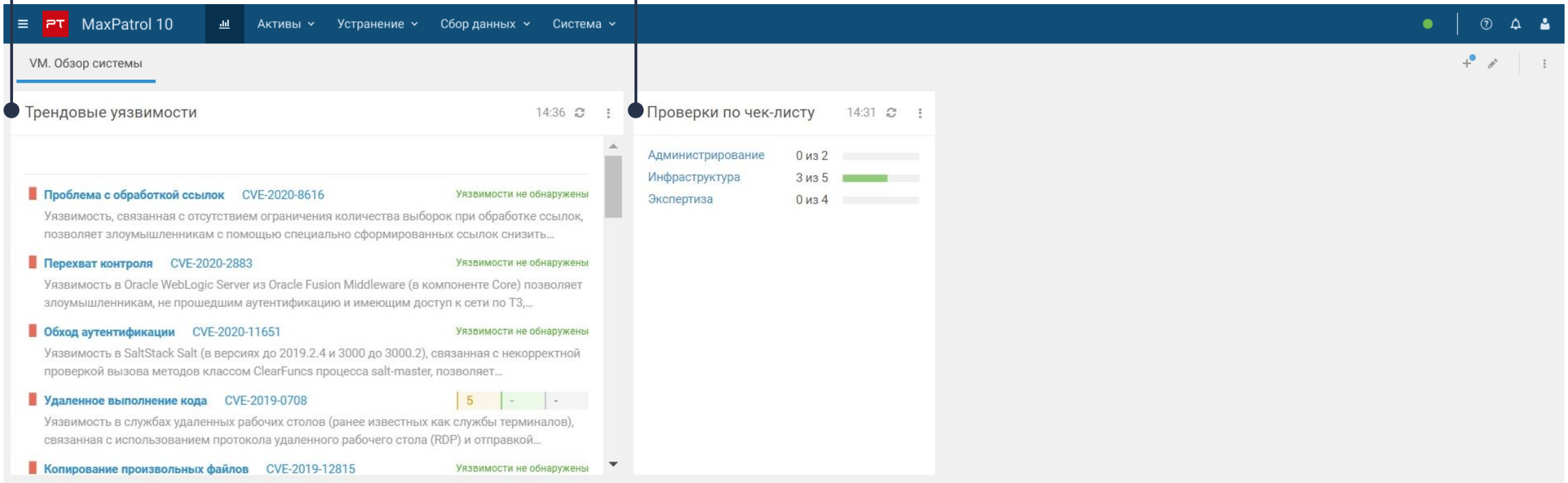
И за нарушением SLA! Контролируй своевременное устранение



MaxPatrol VM

Получай информацию от экспертов PT
о самых трендовых уязвимостях, которые
сейчас используют хакеры и пентестеры

Следи за состоянием
внедрения VM



Зачем нужно
управление активами

ПОЛНЫЙ КОНТРОЛЬ IT-ИНФРАСТРУКТУРЫ

Проблема №1

ИБ-шник не в курсе, какие активы есть в сети

MaxPatrol VM

- Регулярная актуализация данных об активах
- Распределение активов по значимости
- Контроль новых и неоцененных активов

Зачем нужно
управление активами

БЫСТРАЯ ОЦЕНКА НАЛИЧИЯ ОПАСНОЙ УЯЗВИМОСТИ

Проблема №2

Нет возможности быстро проверить актуальность уязвимости для инфраструктуры

MaxPatrol VM

- Определение уязвимости без сканирования
- Пассивное сканирование
- Хранение истории актива

Зачем нужен
контроль политик

МЕНЯЕМ ПОДХОД К УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

Проблема №3

Нужно постоянно объяснять IT-отделу необходимость устранения уязвимости

MaxPatrol VM

- Выстраивание прозрачных отношений с IT-отделом
- Фиксация политик регулярного обновления ОС и ПО
- Контроль устранения уязвимостей

Что дает
выстраивание процесса VM

МАКСИМАЛЬНО ЗАТРУДНИТЬ ПРОНИКНОВЕНИЕ В СЕТЬ

Проблема №4

Непонятно, как поставить
правильную цель
в управлении уязвимостями
и добиться ее выполнения

MaxPatrol VM

- Видно текущее состояние защищенности сети
- Список наиболее актуальных и опасных уязвимостей
- Контроль значимых активов

Возможности MaxPatrol VM

ДЕТАЛЬНО ЗНАЕТ IT-ИНФРАСТРУКТУРУ

MaxPatrol VM собирает наиболее полную информацию об активах в базу. Она пополняется за счет сканирования и импорта данных из различных источников: внешних каталогов и других ИБ-решений. Информация не дублируется и привязывается к одному конкретному активу.

ПОМОГАЕТ ВЫСТРОИТЬ ПРОЦЕСС

За счет классификации активов и внедрения политик сканирования и устранения уязвимостей MaxPatrol VM помогает правильно приоритизировать работу над уязвимостями, а также вовремя оценить какие действия влияют на состояние защищенности IT-инфраструктуры.

КОНТРОЛИРУЕТ ЗАЩИЩЕННОСТЬ

MaxPatrol VM отслеживает динамику показателей регулярных сканирований, эта информация поможет контролировать качество сканирования. Также с помощью ретроспективного анализа можно оценить прогресс по устранению уязвимостей, контролировать соблюдение политик и степень защищенности инфраструктуры.

Преимущества MaxPatrol VM

Часть единой платформы безопасности

Все продукты в составе платформы MaxPatrol 10 работают на единой технологии. Продукты легко подключаются и взаимодействуют друг с другом.

Глубокое понимание IT-инфраструктуры

Благодаря уникальной технологии управления активами достигается полная прозрачность сети.

Гибкая настройка системы

MaxPatrol 10 VM позволяет выстроить процесс управления уязвимостями в зависимости от существующих систем и политик безопасности в компании.

Контракт между IT- и ИБ- отделами

Заданные политики по сканированию и управлению уязвимостям наглядно демонстрируют совместную работу ИБ и IT-отделов.

Поддержка экспертов

Команда экспертов Positive Technologies уведомляет о самых актуальных и критичных уязвимостях для экстренной проверки сети

Максимальная автоматизация

Средства автоматизации (динамическая группировка активов, установка триггеров) позволяют повысить точность получаемой информации, экономить ресурсы и свести к минимуму влияние человеческого фактора.

MaxPatrol VM
принцип работы

ptsecurity.com

Обнаружение активов

СБОР ДАННЫХ ОБ IT-ИНФРАСТРУКТУРЕ, ПОСТОЯННАЯ АКТУАЛИЗАЦИЯ

Обновление базы активов:

- Сканирование blackbox и whitebox
- Импорт данных из внешних каталогов (AD, SCCM, гипервизоры)
- Из событий SIEM, NTA

Контроль изменений — появления новых сетевых узлов и служб, переустановки ОС, изменений аппаратной конфигурации; контроль целостности

Контроль полноты данных об активах:

- Выборочное и точечное сканирование активов
- Импорт данных об активах из внешних каталогов
- Контроль ошибок по задачам сканирования
- Контроль активов с неполной информацией
- Контроль недавно обнаруженных активов
- Контроль потенциально удаленных активов

Идентификация активов:

Запатентованный алгоритм, опирается на параметры актива:

- FQDN
- MAC и IP-адреса
- Тип ОС
- Имя сетевого узла
- Признаки виртуальности узла

Управление активами

КЛАССИФИКАЦИЯ И ОЦЕНКА АКТИВОВ

Классификация активов:

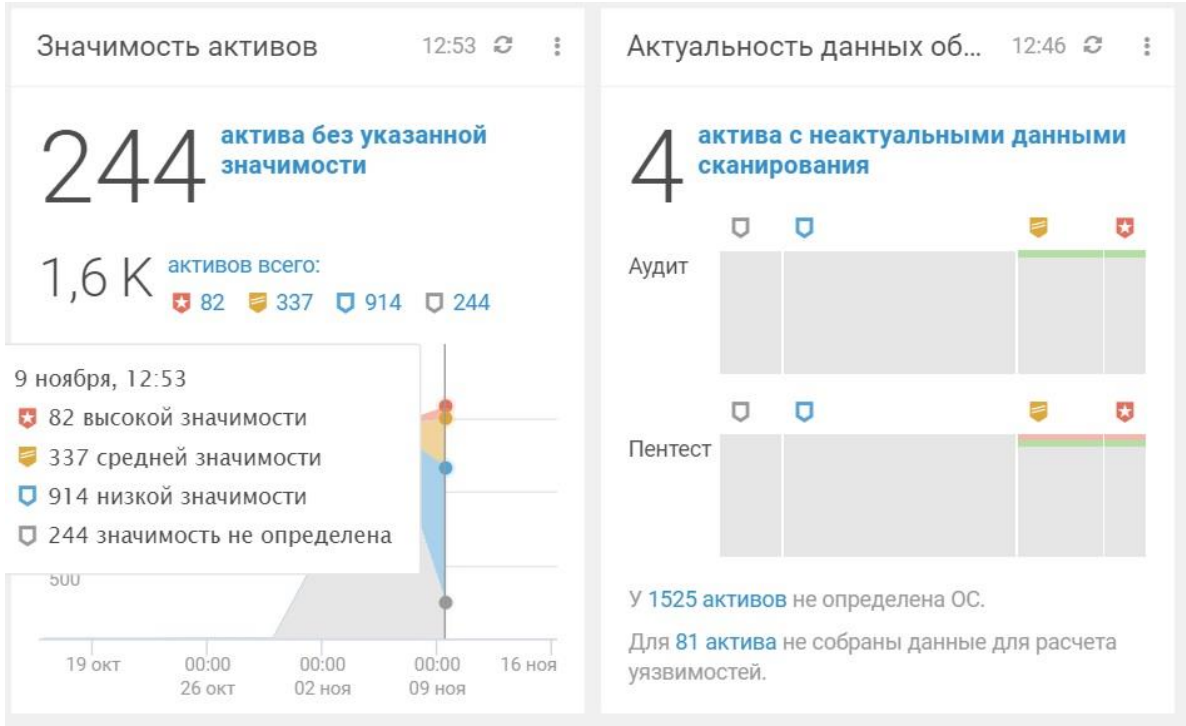
- Динамические группы
- Статические группы
- Триггеры для контроля изменений состава групп

Распределение активов по группам:

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

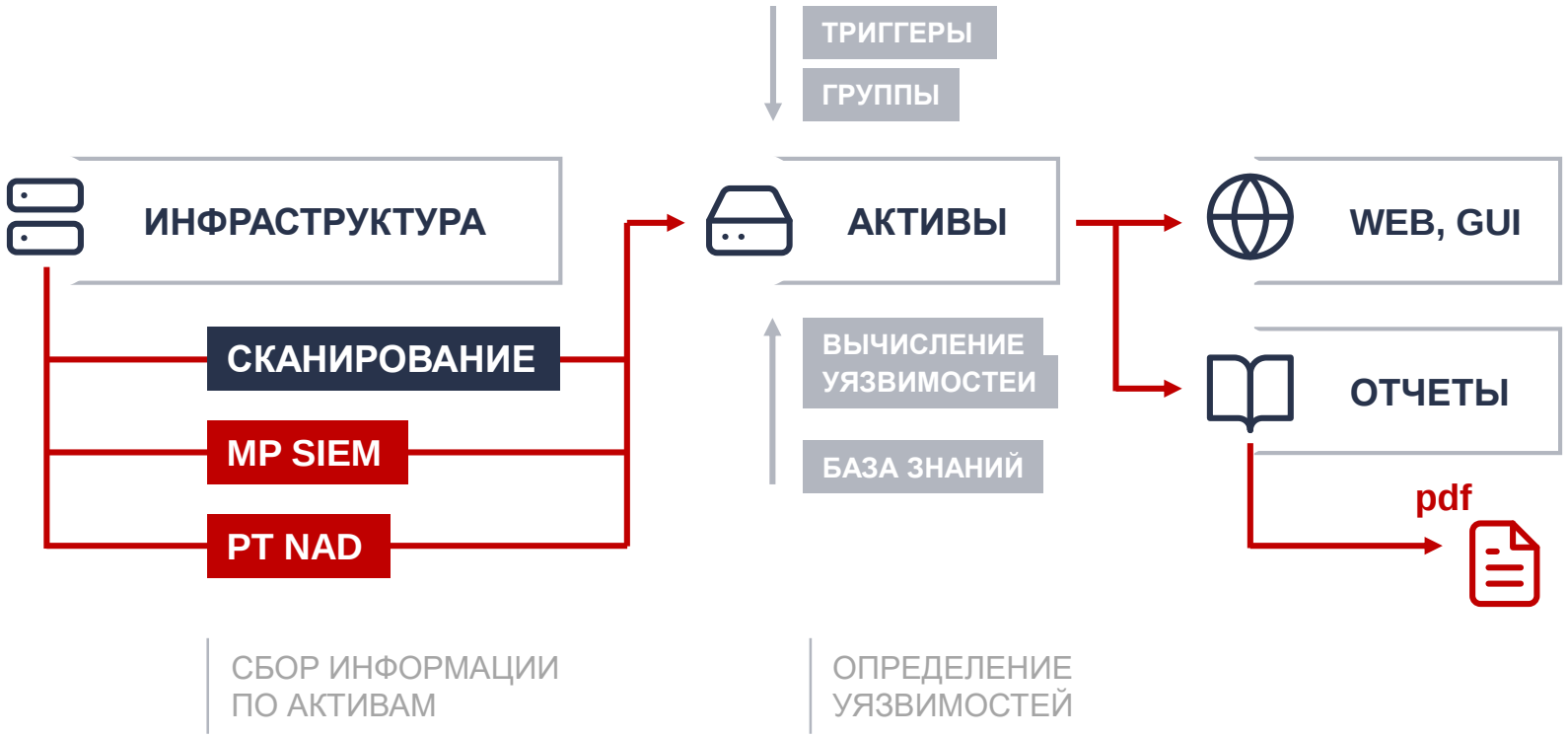
Контроль активов:
их классификации, оценки, регулярности сканирования и устаревания

Оценка активов:
Задание степени важности



Определение уязвимостей

ОПРЕДЕЛЕНИЕ УЯЗВИМОСТЕЙ И ПРАВИЛ ИХ ОБРАБОТКИ



ОПРЕДЕЛЕНИЕ УЯЗВИМОСТЕЙ:

- на основании сканирования в режимах Pentest и Audit
- без сканирования (расчет уязвимостей после обновления базы знаний)
- по правилам, заданным в базе знаний
- пассивное выявление уязвимостей

ОПРЕДЕЛЕНИЕ ПРАВИЛ ОБРАБОТКИ

- понять под автоматический или ручной процесс попадает уязвимость
- Настроить правила автоматизации

Работа с уязвимостями

КЛАССИФИКАЦИЯ И ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ

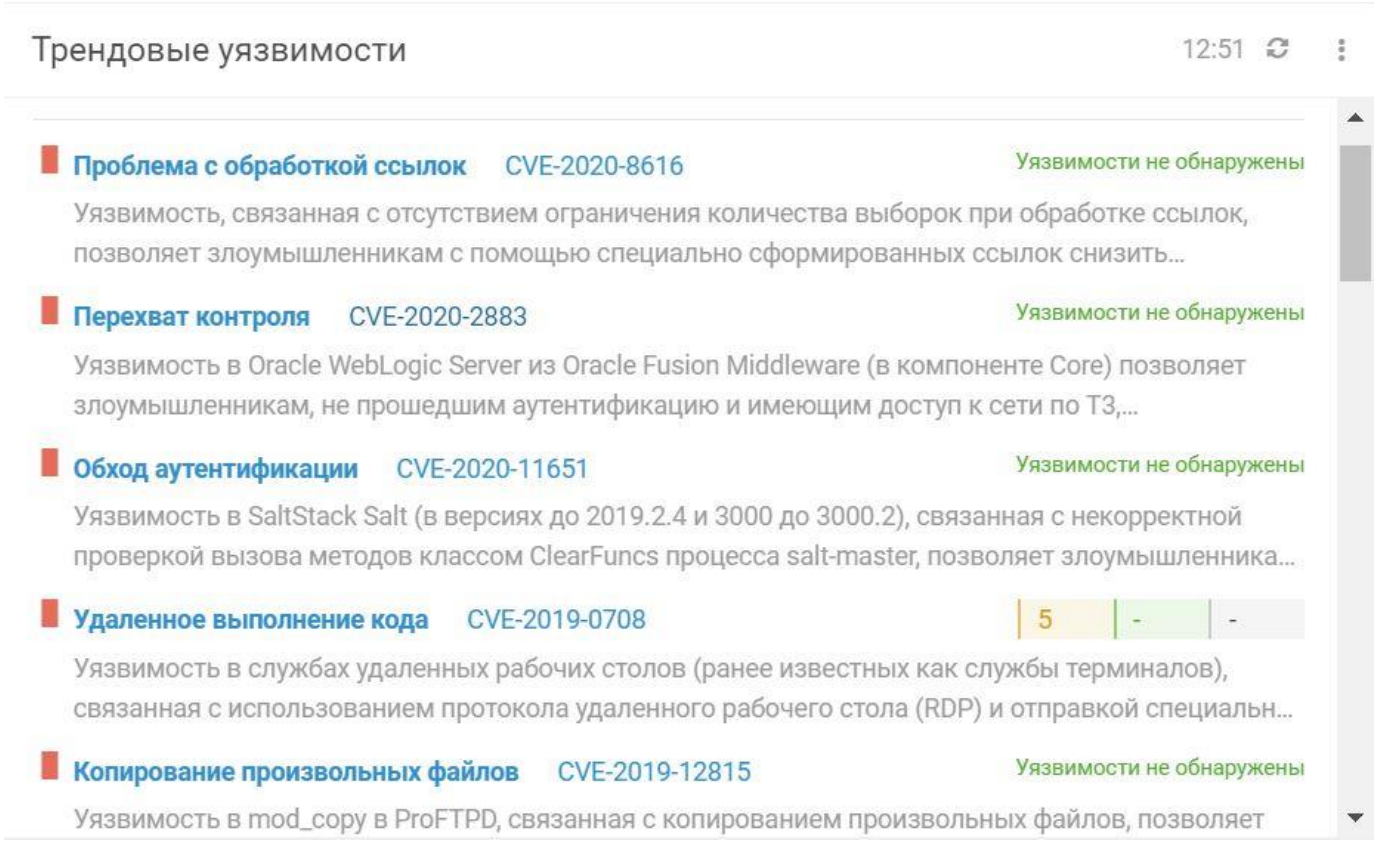
- Задание политик для планового устранения специалистами IT

- **Фильтрация уязвимостей**

  при ручном разборе:

  - Активы особой важности
  - Уязвимости, не покрытые политиками
  - Неустранимые уязвимости (тех ограничения)
  - 0-day

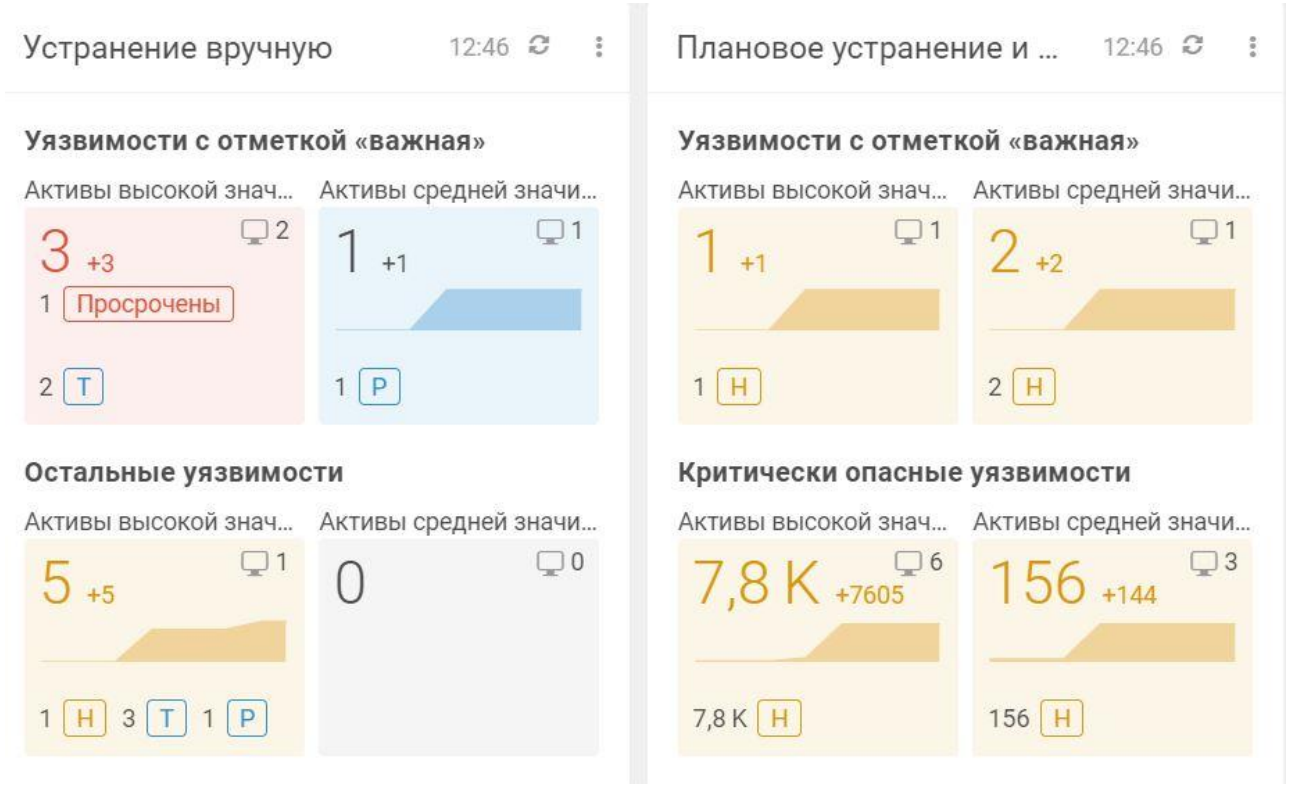
- **Трендовые уязвимости**
  Подбор наиболее актуальных и критичных уязвимостей



Контроль устранения уязвимостей

ОЦЕНКА СОБЛЮДЕНИЯ ПОЛИТИК И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

- Задание **сроков устранения уязвимостей** в зависимости от их типа и важности активов
- Отслеживание динамики наличия **просроченных уязвимостей**, отдельная статистика по ООУ
- **Ретроспективный анализ** устранения уязвимостей помогает понять: нужные ли уязвимости устранялись и на тех ли активах велись работы



Интеграция
с другими системами

ptsecurity.com

Возможности интеграции

MaxPatrol VM
интегрируется с другими системами, что позволяет получить дополнительные сведения об активах и сделать перерасчет уязвимостей

MaxPatrol SIEM

Система выявления инцидентов ИБ

Данные об обнаруженных активах постоянно дополняются информацией из систем анализа событий и инцидентов ИБ. Это дает актуальную картину IT-инфраструктуры.

PT Network Attack Discovery

Система глубокого анализа сетевого трафика (NTA)

База активов обогащается информацией о сетевых соединениях. Для поиска новых уязвимостей собираются данные также из трафика. Это позволяет выявлять уязвимости внутри инфраструктуры.

Как начать работу
с MaxPatrol VM

ptsecurity.com

Как провести «пилот» MaxPatrol VM

Заявка
Оставьте заявку на нашем сайте

Подписание NDA, заполнение анкеты, составление плана

Развертывание MaxPatrol VM: установка, настройка

Пилотный проект, мониторинг специалистами Positive Technologies

Отчет об уровне защищенности инфраструктуры

≈ 4 недели

План пилота

ЧТО БУДЕМ ДЕЛАТЬ

РЕЗУЛЬТАТ

- Построили процесс управления уязвимостями
- Показали оперативную работу с трендовыми уязвимостями
- Выявлен ТОП уязвимых активов
- Увидели динамику устранения уязвимостей
- Проверили договоренности с IT

MAXPATROL VM

ВЫСТРОИТ ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ, РЕЗУЛЬТАТЫ КОТОРОГО ВИДНЫ

Чат в Телеграмме:
t.me/MPSIEMChat

Вебинары:
www.ptsecurity.com/ru-ru/research/webinar/

ptsecurity.com