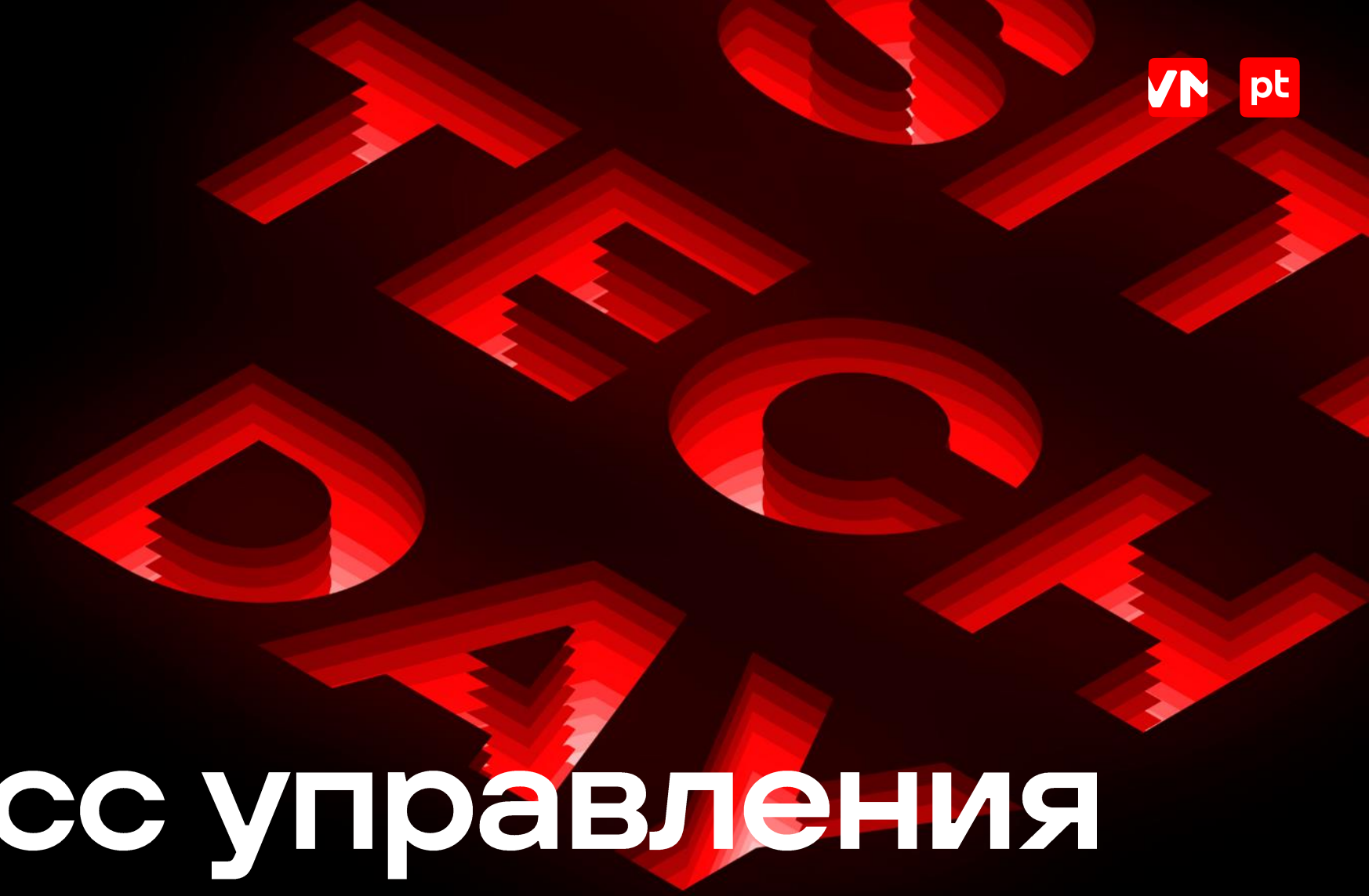
Антон Киселев
Руководитель направления развития продуктов анализа защищенности инфраструктуры

MaxPatrol VM: процессы и тренды

01



Процесс управления уязвимостями

Процесс управления уязвимостями

На что обратить внимание

- Определение требований к процессу
- Требования к ресурсам
- Согласование процесса между всеми участниками и контроль за договоренностями

Процесс управления уязвимостями

Этапы

1

Инвентаризация инфраструктуры

Процесс управления уязвимостями

Этапы

1 Инвентаризация инфраструктуры

2 Категоризация активов

Процесс управления уязвимостями

Этапы

1. Инвентаризация инфраструктуры
2. Категоризация активов
3. Формирование и согласование SLA

Процесс управления уязвимостями

Этапы

1. Инвентаризация инфраструктуры
2. Категоризация активов
3. Формирование и согласование SLA
4. Поиск уязвимостей и их категоризация

Процесс управления уязвимостями

Этапы

1. Инвентаризация инфраструктуры
2. Категоризация активов
3. Формирование и согласование SLA
4. Поиск уязвимостей и их категоризация
5. Контроль за устранением уязвимостей

Процесс управления уязвимостями

Этапы

1. Инвентаризация инфраструктуры
2. Категоризация активов
3. Формирование и согласование SLA
4. Поиск уязвимостей и их категоризация
5. Контроль за устранением уязвимостей
6. Контроль за процессом и совершенствование процесса

Процесс управления уязвимостями

Если есть трендовая уязвимость...

1

CVE-2024-38077
Вендор: Microsoft

2

А она точно есть?

3

А как проверить?

4

Как закрыть?

5

SLA?

6

Результат

Процесс управления уязвимостями

Основные компоненты

Процесс управления уязвимостями — непрерывная, постоянно повторяющаяся активность по поиску уязвимостей и выработке рекомендаций на основе полученных данных.

Процесс управления уязвимостями строится на трех основных компонентах:

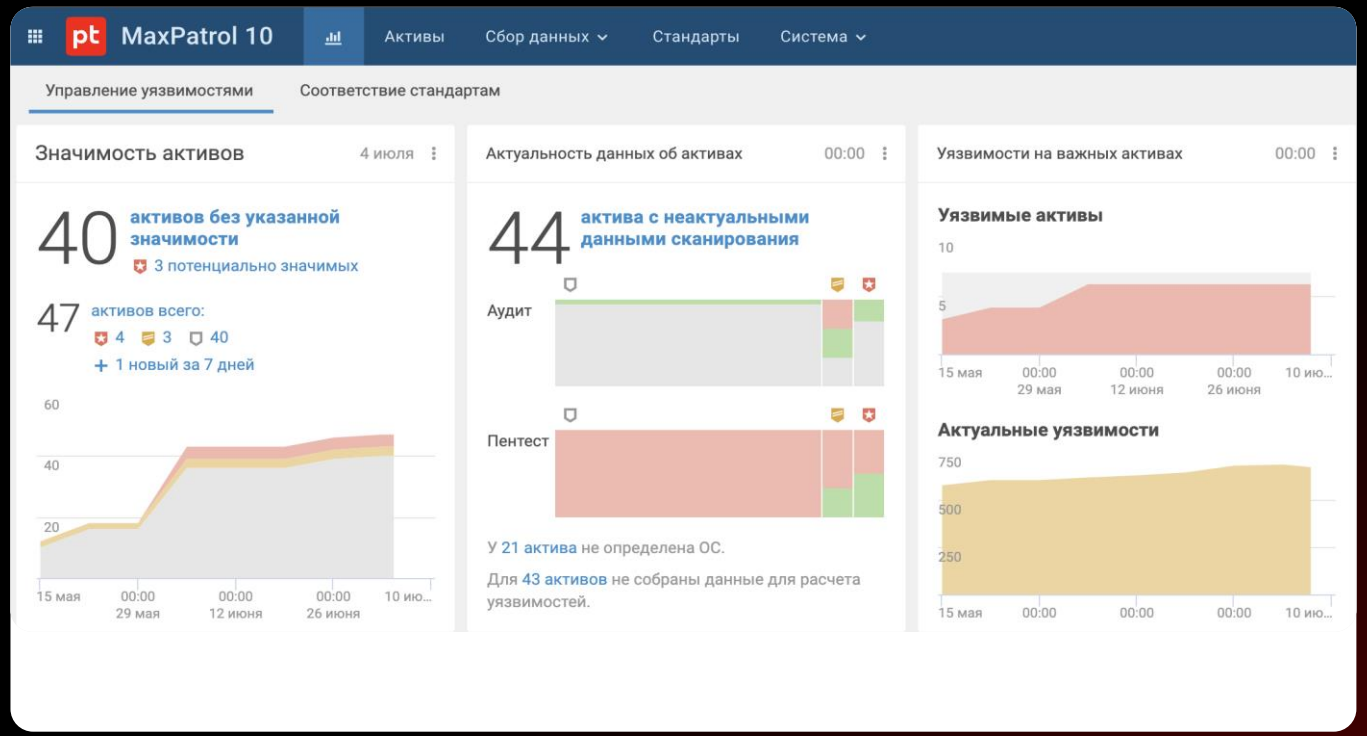
- Продукты
- Люди
- Результаты

02

Решения

MaxPatrol VM

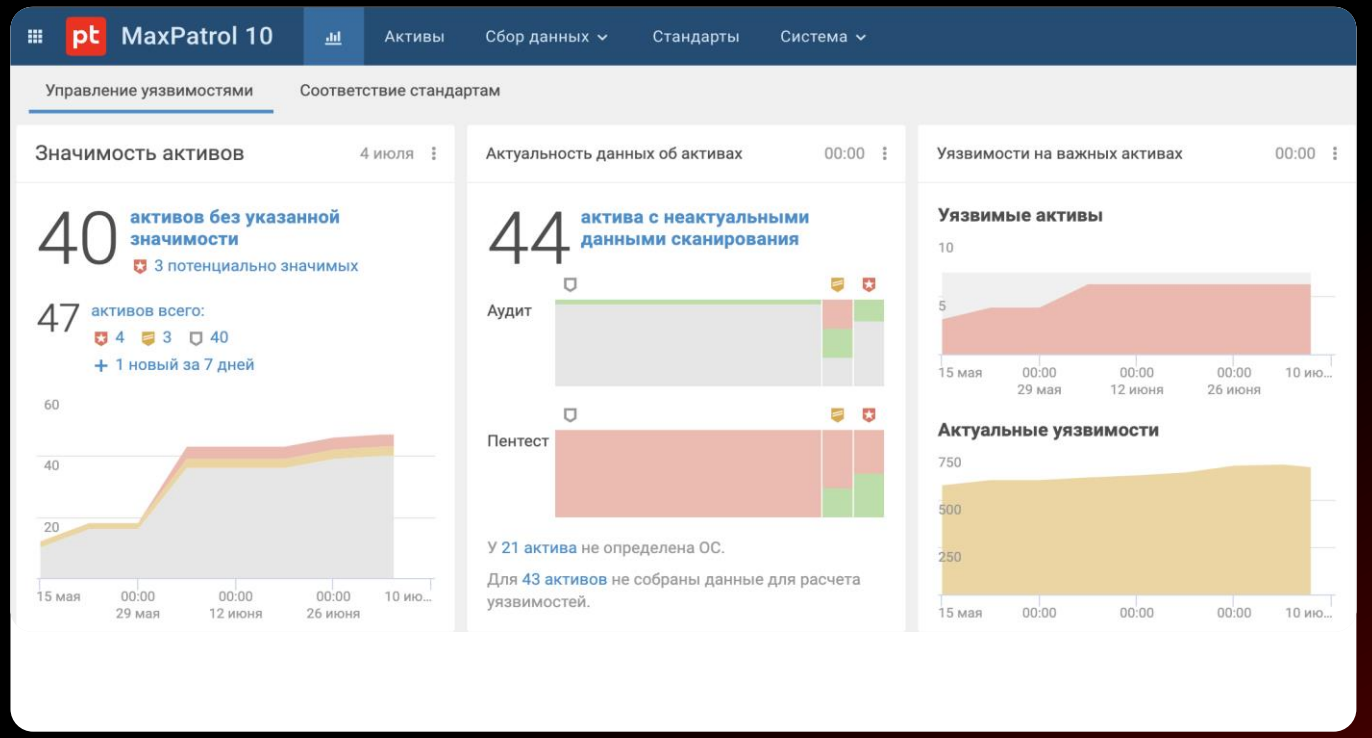
Решение для построения
полноценного
процесса управления
уязвимостями
и для контроля
соответствия стандартам



MaxPatrol VM

Новое из последних релизов

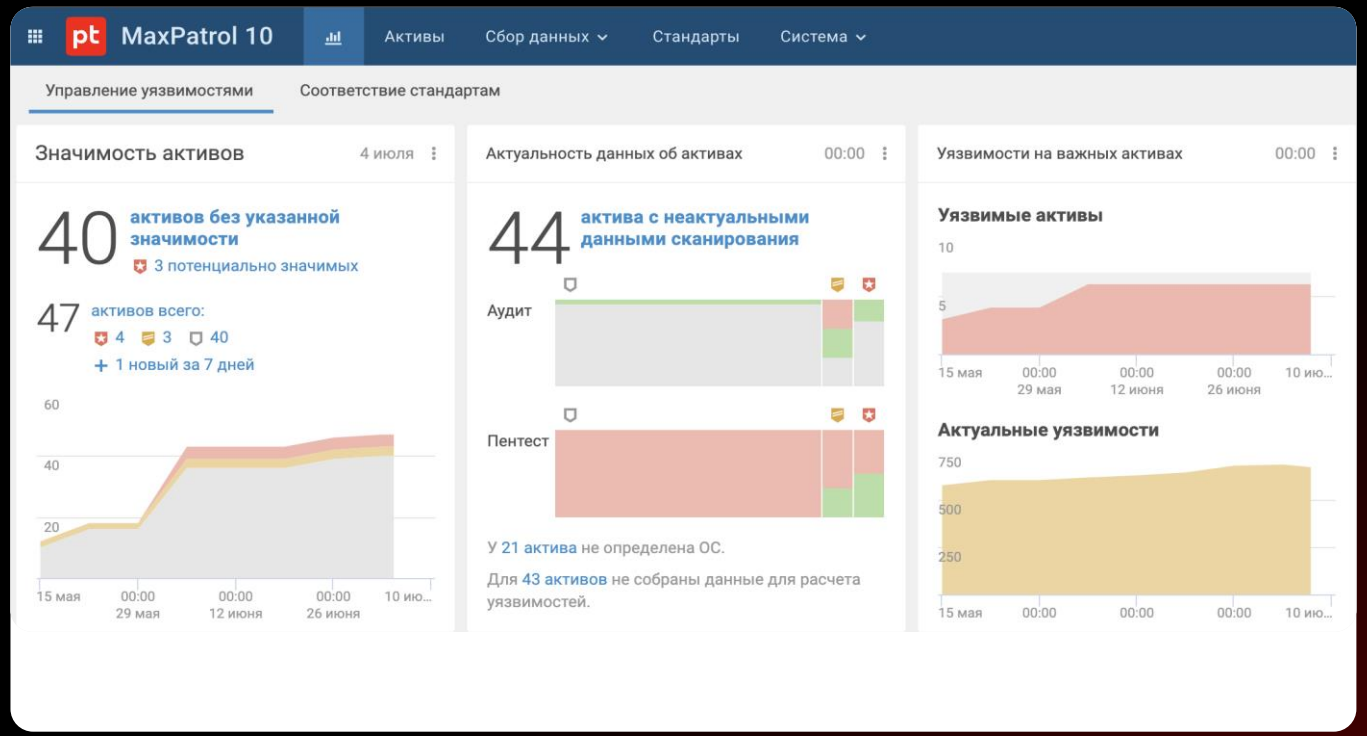
- Управление потоками сканирования и приоритетами
- Визуализация и гибкость отчетов
- Хостовой и сетевой коллекторы
- Контроль стандартов безопасности и их кастомизация
- Ролевая модель доступа к группам



MaxPatrol VM

Новое из последних релизов

- Кастомизация сбора информации об активе
- Технологические окна для сканирования
- Полноценное DAST сканирование WEB
- Сканирование образов запущенных в Docker
- Проверка подключения
- обновление Pentest проверок из облака



MaxPatrol VM

Что у нас впереди

- ML4PDQL
- VM Lite
- Reporting Portal
- Иерархия ядер
- Упрощение установки и обновления продуктов
- Контроль лицензионных метрик

03

Люди

Люди

в процессе управления уязвимостями

Обучение работе с продуктом

Практикум по управлению уязвимостями

04

Результаты

Что будет результатом процесса управления уязвимостями

- Устранение трендовых уязвимостей на критически важных активах в течение...
- Нулевая толерантность к рискам
- SLA выполняется, уязвимости закрываются в срок
- Постоянный рост количества устраненных уязвимостей
- ...

Внимание,
опрос!

Узнать больше
о MaxPatrol VM

Спасибо!