Управление уязвимостями: что должны уметь VM-решения

Антон Исаев
Ведущий специалист отдела развития
и продвижения инженерно-технической
экспертизы Positive Technologies

Challenge 2022

- Уход иностранных производителей с рынка
- Риск "небезопасного" обновления ПО
- Рост количества атак на российские компании

Что должны уметь VM-решения

- Сканирование IT-инфраструктуры
- Анализ результатов сканирования
- Выявление уязвимостей
- Контроль устранения уязвимостей
- Взаимодействие с IT-отделом

Сканирование IT-инфраструктуры

Регулярная актуализация базы активов

Контроль полноты собранных данных

Контроль изменений в инфраструктуре

Сбор данных

- Host Discovery
- * Discovery
- * Pentest

- Windows Updates Discovery
- * Audit

- AD
- SCCM
- VmWare vCenter

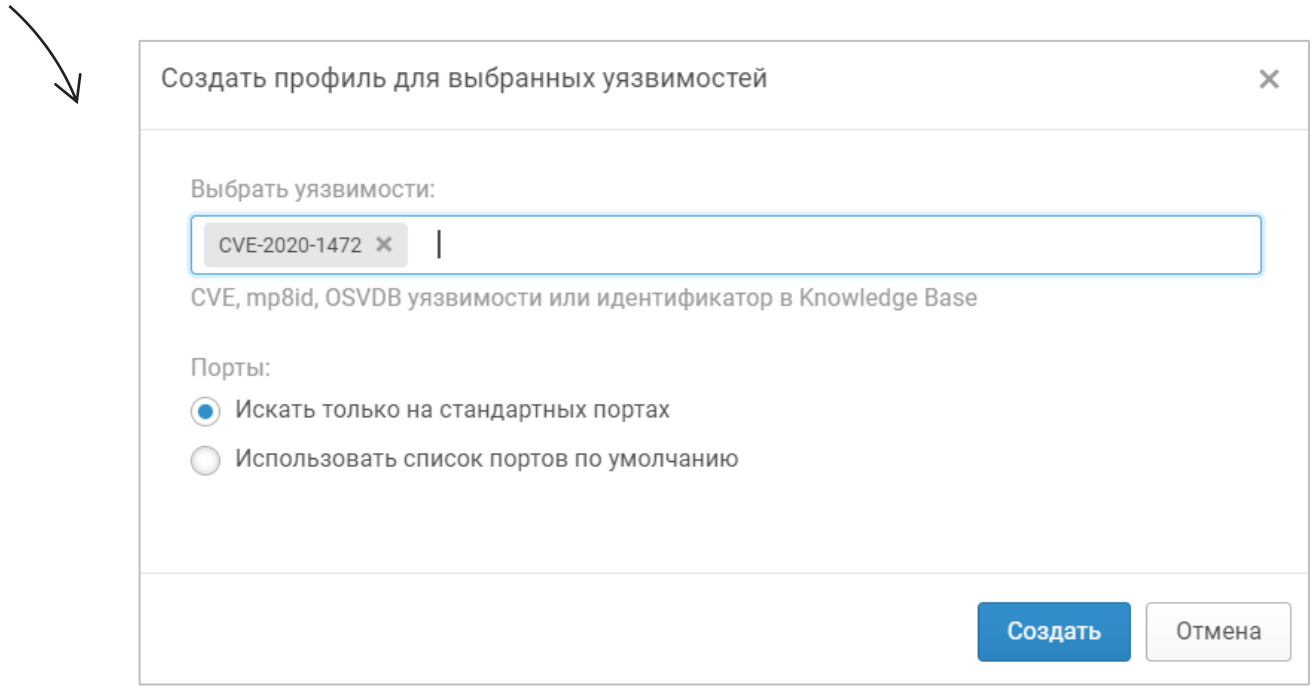
SIEM

- DHCP servers
- DNS servers
- Checkpoint, Cisco
- Kaspersky Security Center
- другие

- PT NAD

ПРИМЕР №1

Смотрим, где в сети есть **Zerologon**: создаем точечный профиль с CVE-2020-1472



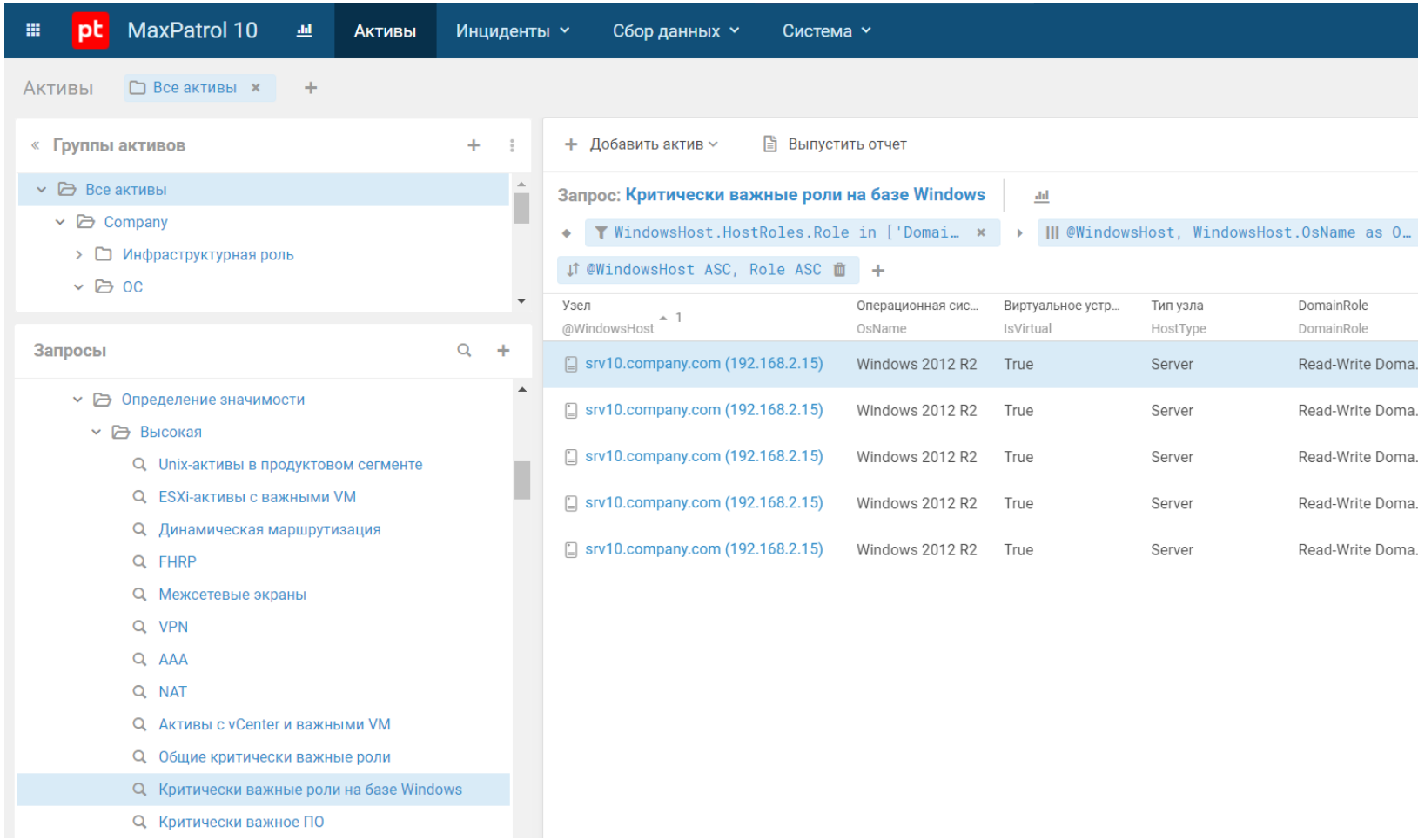
Анализ результатов сканирования

Оценка активов по значимости для бизнес-процессов компании

Классификация и распределение активов по группам для автоматизации работы

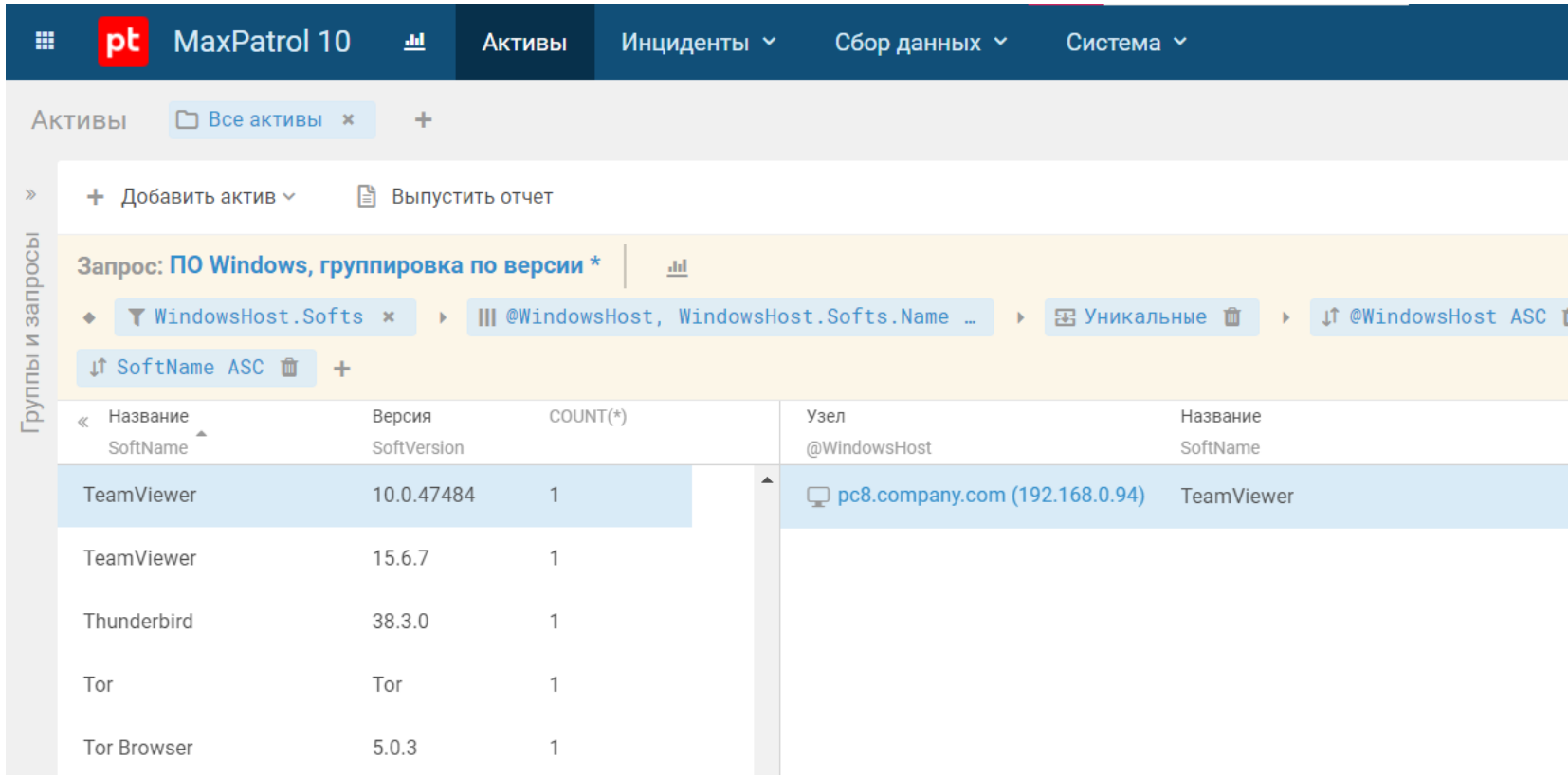
ПРИМЕР №2

Задаем всем контроллерам домена высокую значимость



ПРИМЕР №3

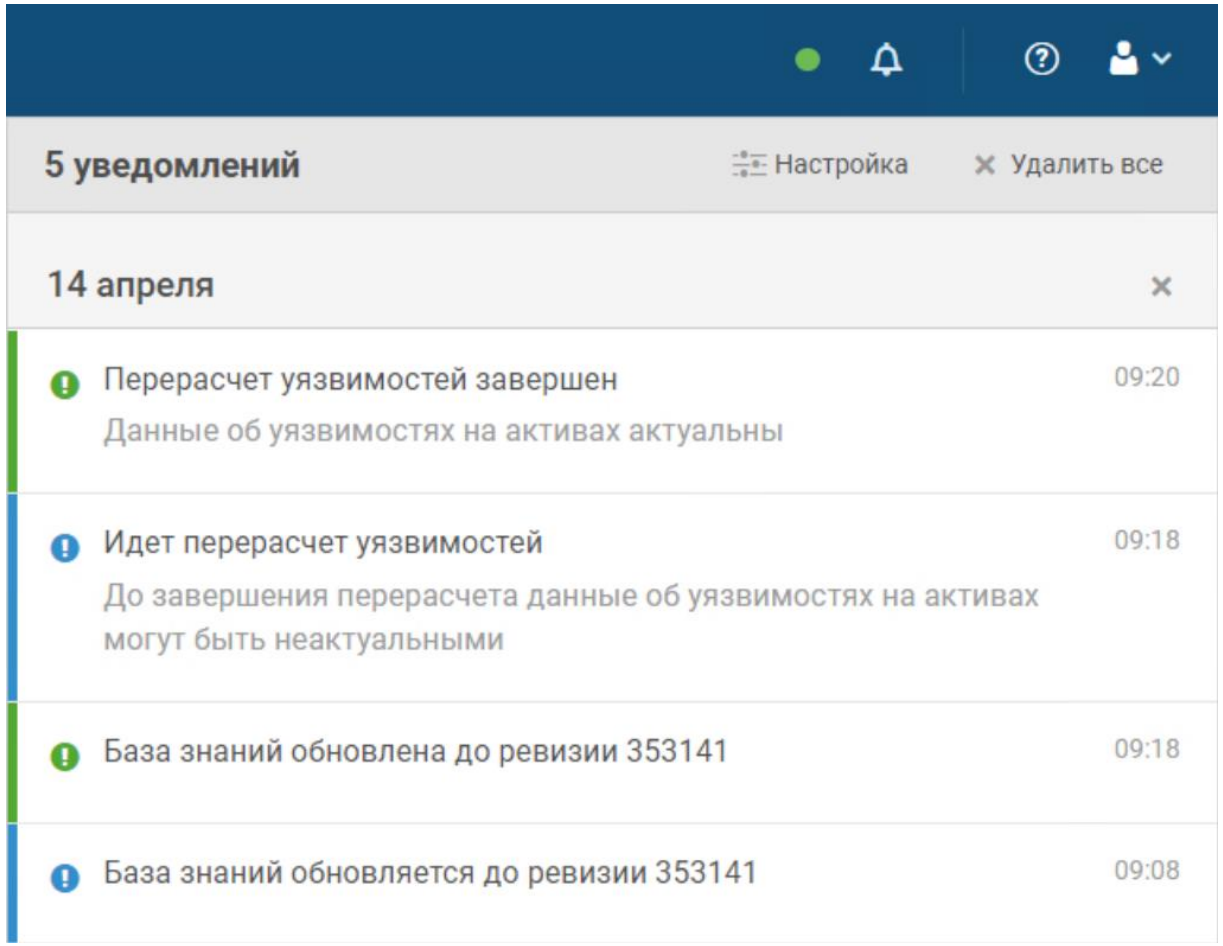
Находим нелегитимное или устаревшее ПО



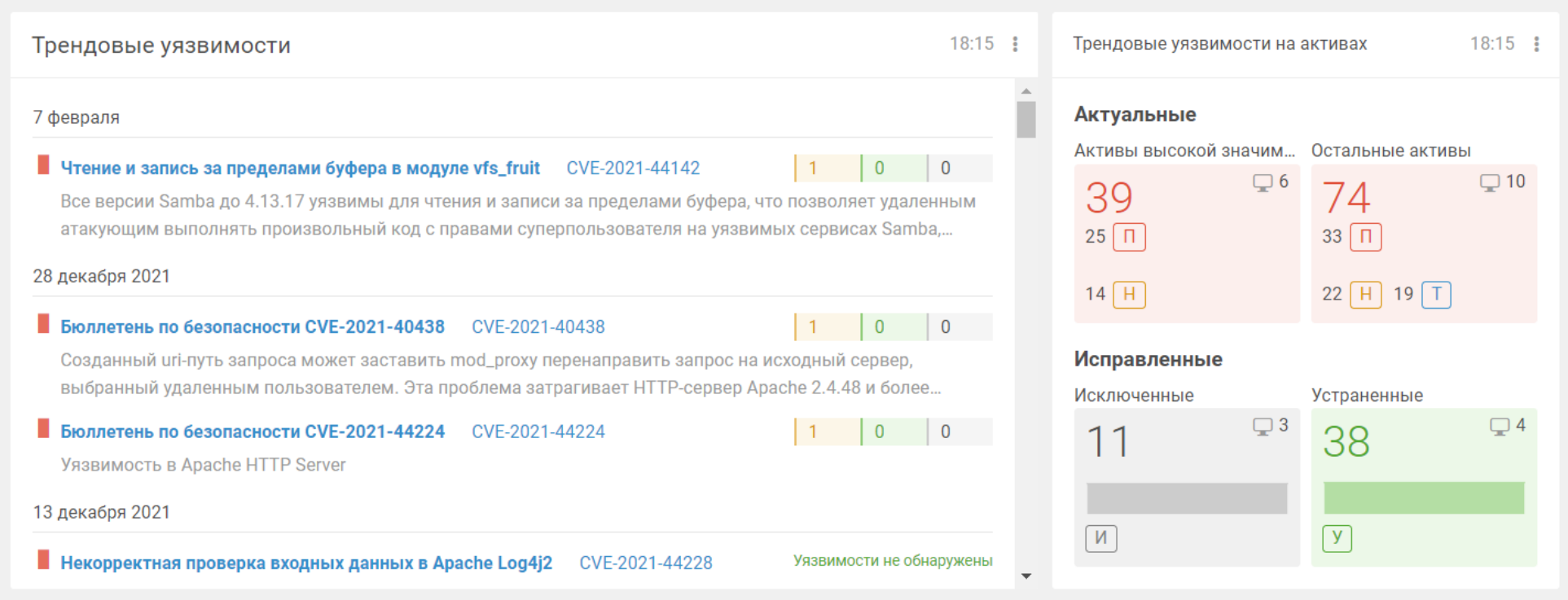
Выявление уязвимостей

- Фокус на самых опасных уязвимостях
- Контроль состояния активов высокой значимости
- Быстрое реагирование на новые опасные уязвимости

Выявления уязвимостей без повторного сканирования
Информация об уязвимостях актуализируется автоматически после обновления базы знаний



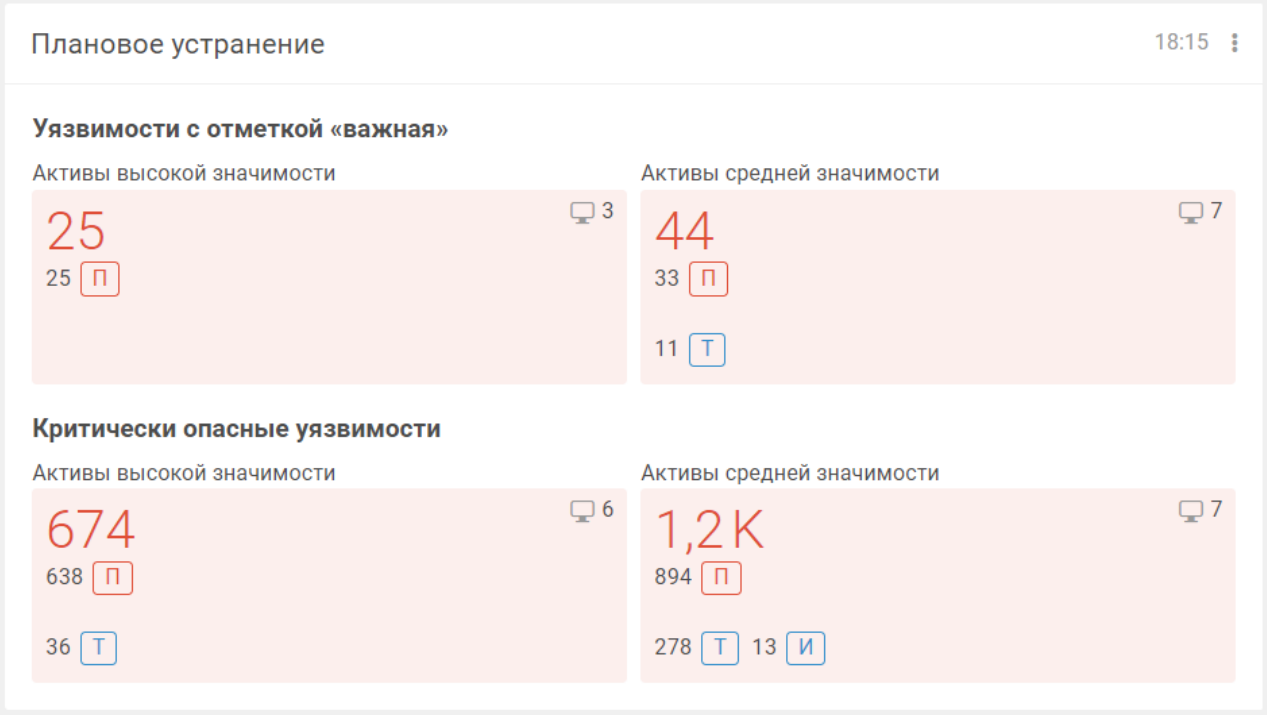
Трендовые уязвимости
Популярны у злоумышленников. Их нужно устранить в первую очередь

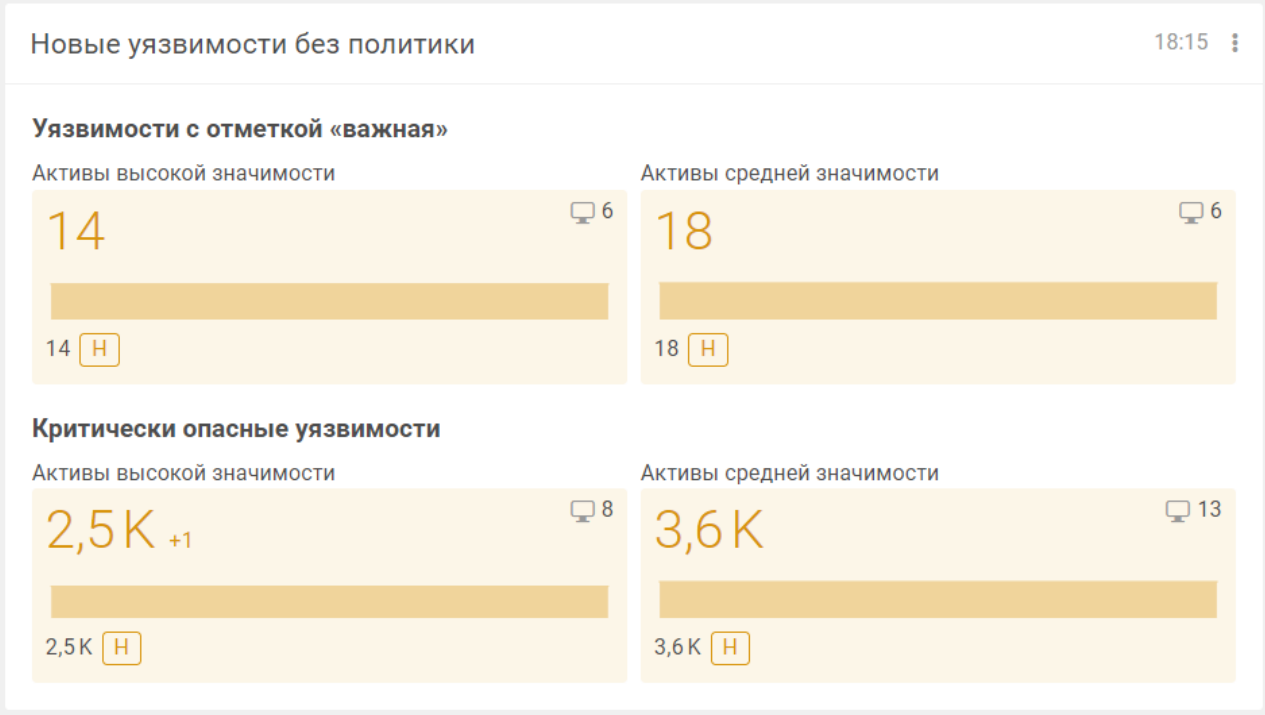


Построение процесса VM

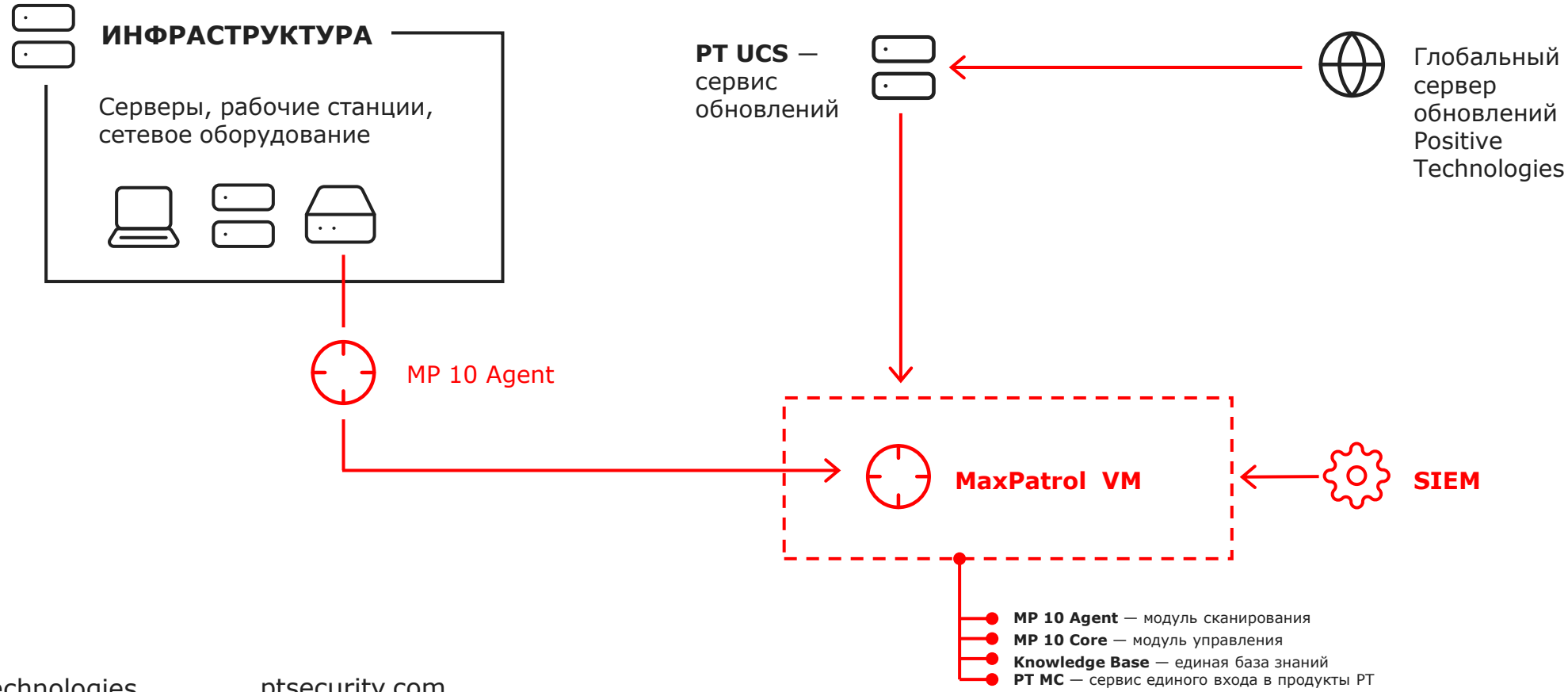
- Фиксация политик регулярного обновления ОС и ПО
- Контроль устранения уязвимостей
- Выстраивание прозрачных отношений с IT-отделом

Построение процесса VM

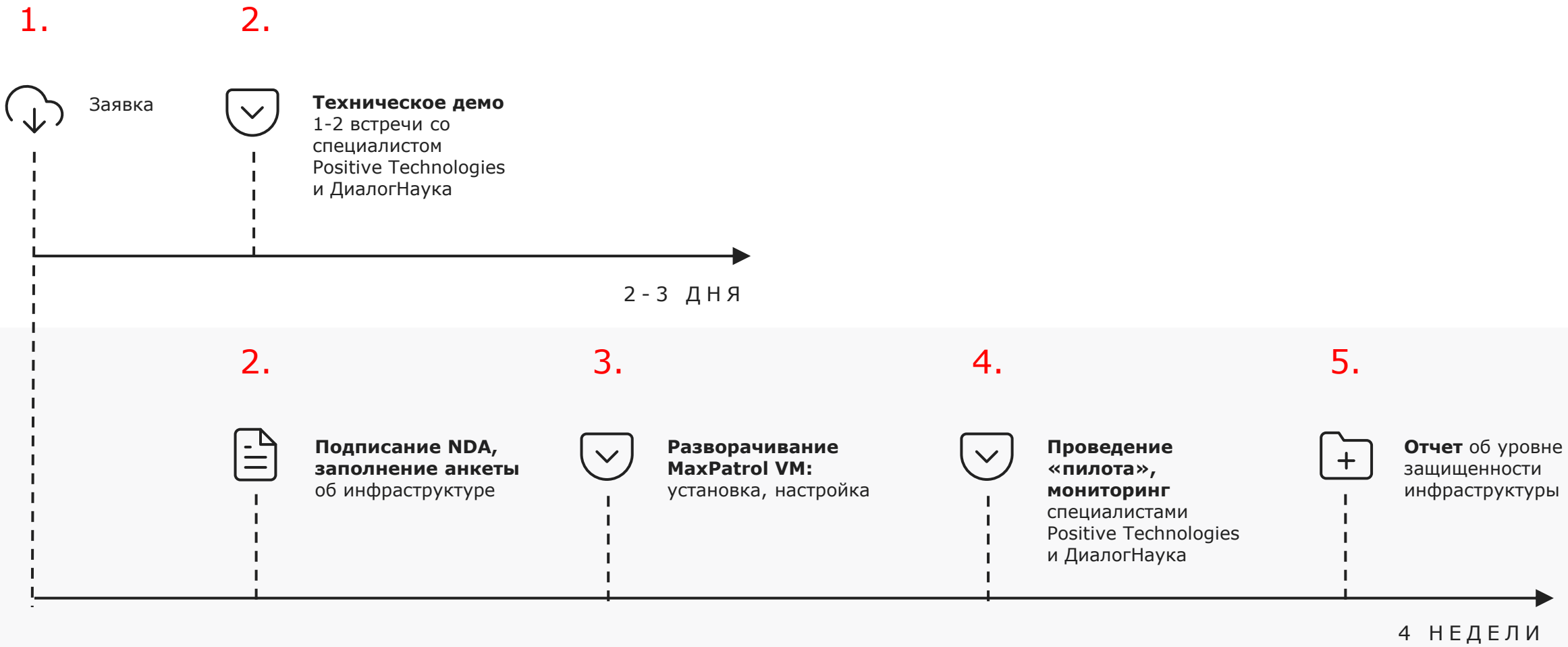




Архитектура MaxPatrol VM



Как попробовать MaxPatrol VM



Спасибо за внимание

- Телеграм-канал с новостями продуктов Positive Technologies: t.me/ptproductupdate

- Задать вопрос о функционале MaxPatrol 10: t.me/MPSIEMChat