



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



Создать профиль для выбранных уязвимостей ×

Выбрать уязвимости:

CVE-2020-1472 × |

CVE, mp8id, OSVDB уязвимости или идентификатор в Knowledge Base

Порты:

Искать только на стандартных портах

Использовать список портов по умолчанию

Создать Отмена

Анализ результатов сканирования



Оценка активов по значимости для бизнес-процессов компании



Классификация и распределение активов по группам для автоматизации работы

ПРИМЕР №2

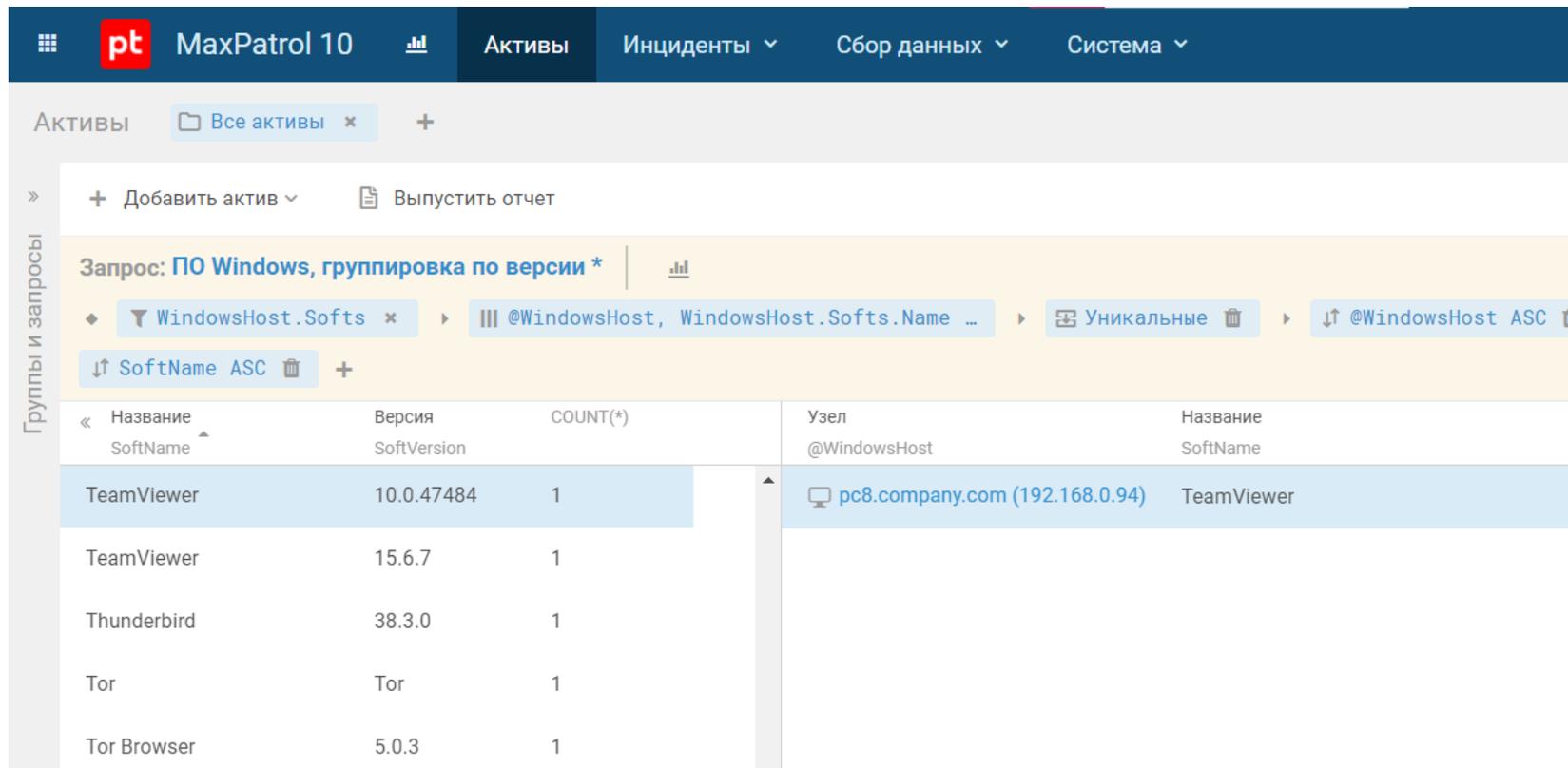
Задаем всем
контроллерам домена
высокую значимость

The screenshot shows the MaxPatrol 10 interface. The top navigation bar includes 'Активы', 'Инциденты', 'Сбор данных', and 'Система'. The main content area is divided into several sections:

- Группы активов:** A tree view showing 'Все активы' expanded to 'Company', which contains 'Инфраструктурная роль' and 'ОС'.
- Запросы:** A list of saved queries under 'Определение значимости' and 'Высокая'. The query 'Критически важные роли на базе Windows' is selected.
- Search Results:** A table displaying the results of the selected query. The table has columns: Узел, Операционная сис..., Виртуальное устр..., Тип узла, and DomainRole. The results show five entries for 'srv10.company.com (192.168.2.15)' with 'Windows 2012 R2' OS, 'True' for 'IsVirtual', and 'Server' for 'HostType'. All entries have 'Read-Write Doma...' as the 'DomainRole'.

ПРИМЕР №3

Находим нелегитимное
или устаревшее ПО



Макет интерфейса MaxPatrol 10. Вкладка «Активы». Поиск: ПО Windows, группировка по версии. Результаты поиска:

Название	Версия	COUNT(*)	Узел	Название
SoftName	SoftVersion		@WindowsHost	SoftName
TeamViewer	10.0.47484	1	pc8.company.com (192.168.0.94)	TeamViewer
TeamViewer	15.6.7	1		
Thunderbird	38.3.0	1		
Tor	Tor	1		
Tor Browser	5.0.3	1		

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

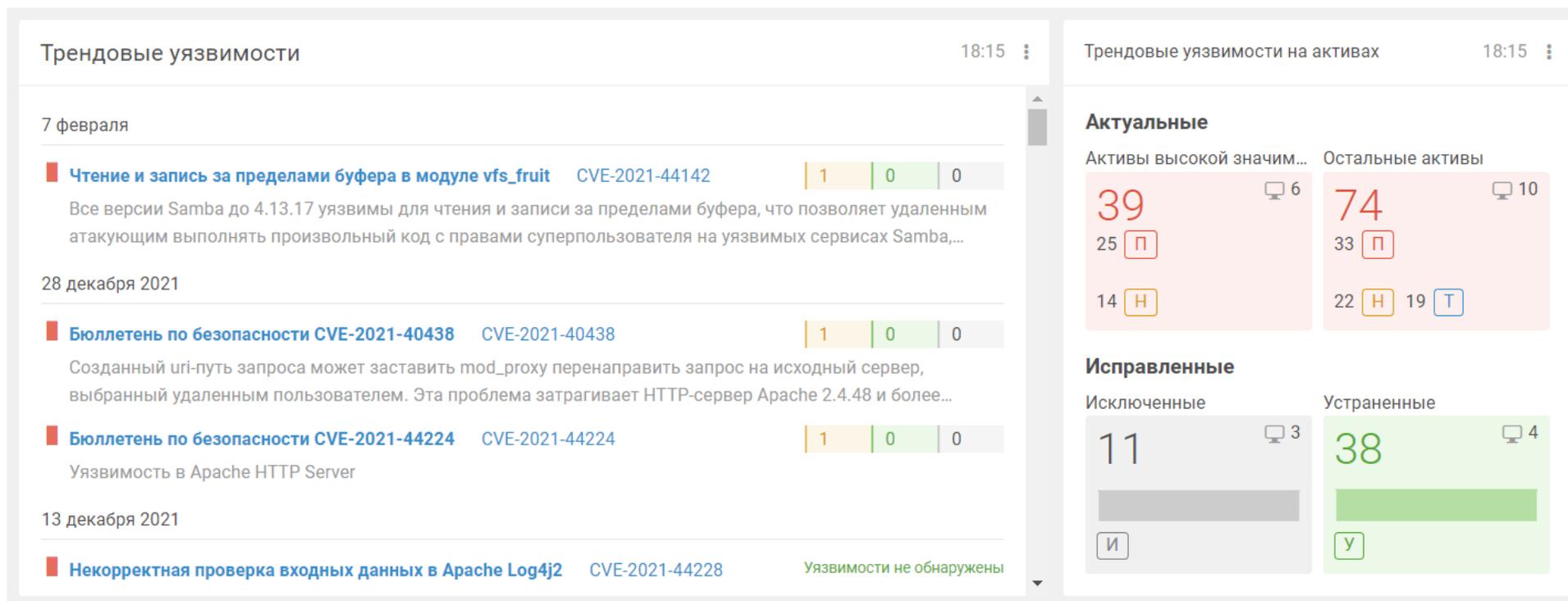


5 уведомлений Настройка Удалить все

14 апреля ×

- ! Перерасчет уязвимостей завершен 09:20
Данные об уязвимостях на активах актуальны
- ! Идет перерасчет уязвимостей 09:18
До завершения перерасчета данные об уязвимостях на активах могут быть неактуальными
- ! База знаний обновлена до ревизии 353141 09:18
- ! База знаний обновляется до ревизии 353141 09:08

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

Плановое устранение

18:15

Уязвимости с отметкой «важная»

Активы высокой значимости

25

25 П

3

Активы средней значимости

44

33 П

11 Т

7

Критически опасные уязвимости

Активы высокой значимости

674

638 П

36 Т

6

Активы средней значимости

1,2K

894 П

278 Т 13 И

7

Новые уязвимости без политики

18:15

Уязвимости с отметкой «важная»

Активы высокой значимости

14

14 Н

6

Активы средней значимости

18

18 Н

6

Критически опасные уязвимости

Активы высокой значимости

2,5K +1

2,5K Н

8

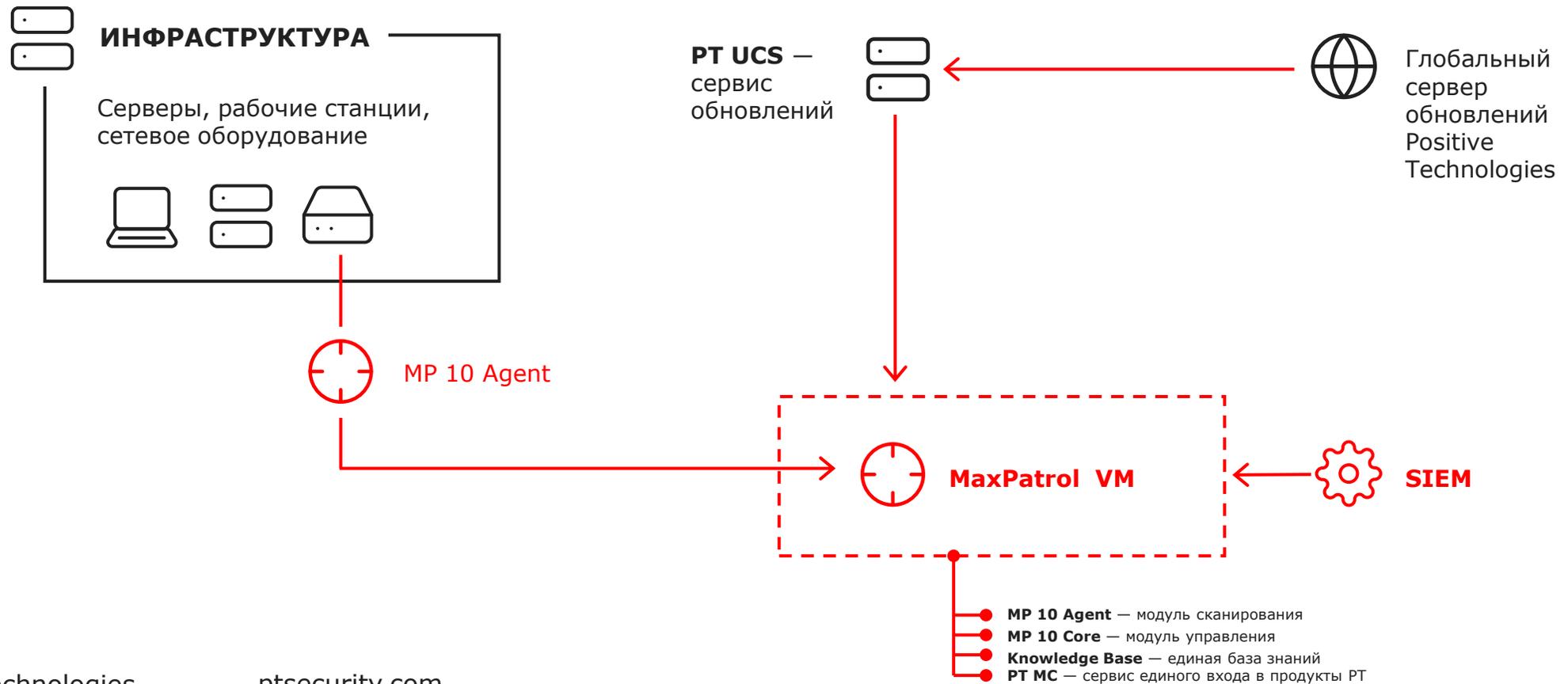
Активы средней значимости

3,6K

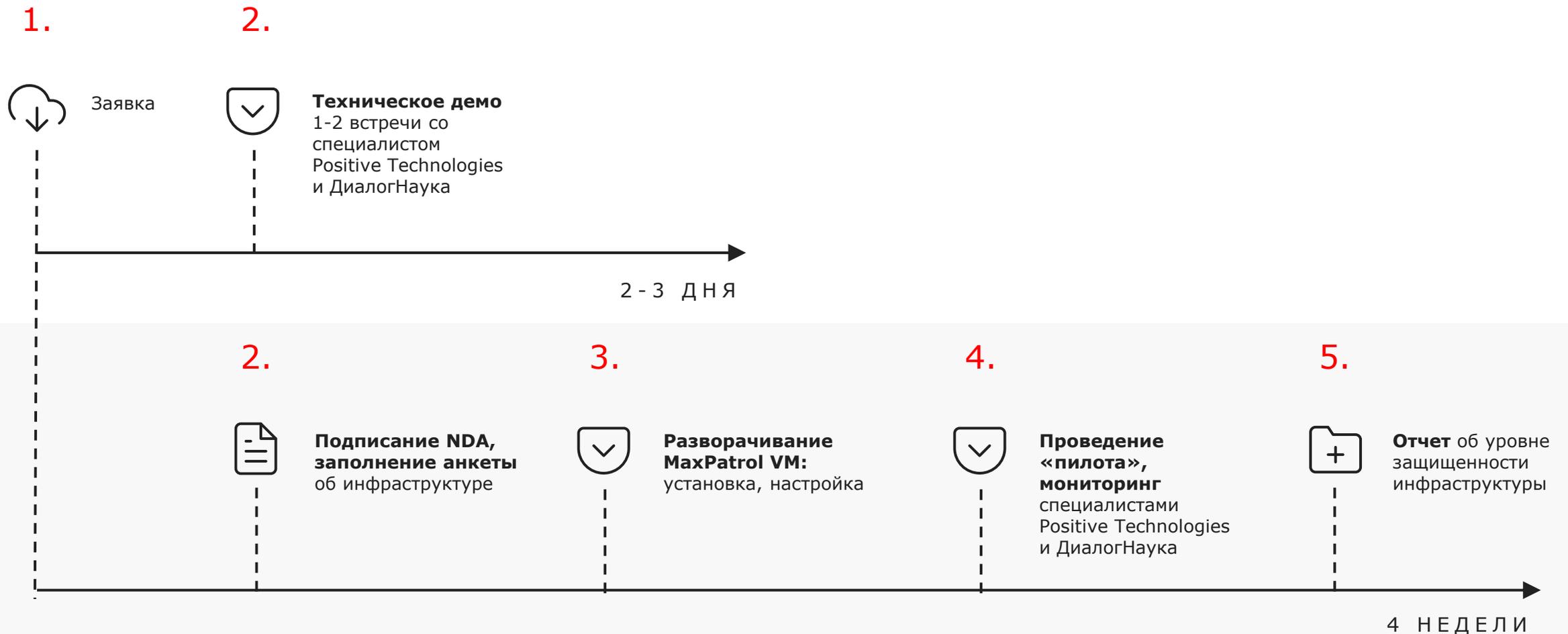
3,6K Н

13

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