POSITIVE TECHNOLOGIES

MaxPatrol VM

Система управления уязвимостями нового поколения

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** не проверяют, устранил ли IT-отдел уязвимости

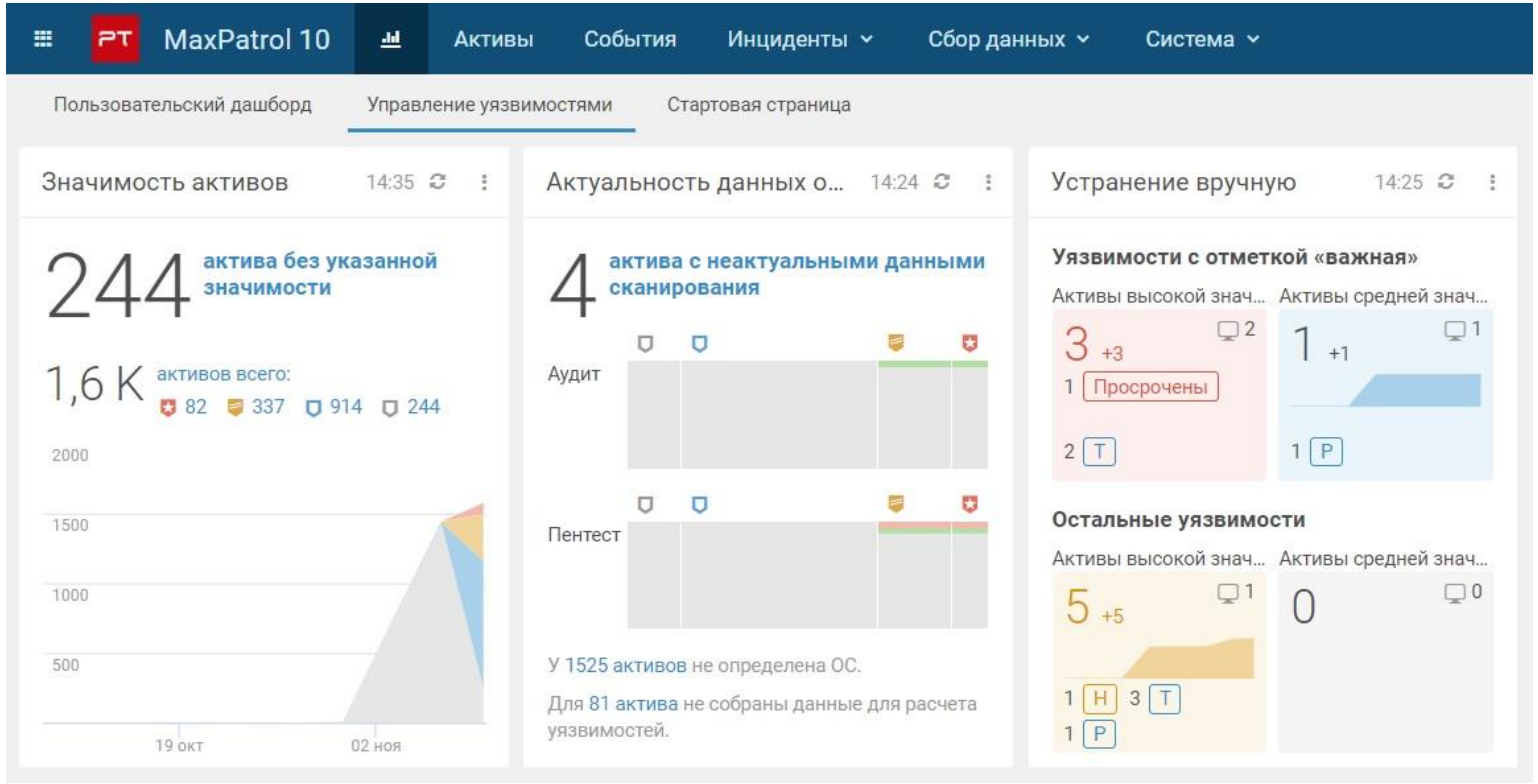
57% **СПЕЦИАЛИСТОВ** в приоритизации уязвимостей доверяют оценке по CVSS

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

Новое решение

MAXPATROL VM

Система управления уязвимостями нового поколения



- Помогает построить полноценный процесс управления уязвимостями
- Отслеживает трендовые уязвимости
- Помогает создать контракт между ИБ и IT-отделами
- Является частью единой платформы безопасности

Общий процесс VM

Обработка Особо Опасных

Почему MP VM другой?

MaxPatrol VM:

- это не новая версия MaxPatrol 8
- это не сканер уязвимостей с интеграцией в тикет-систему
- это точно не сканер!

MaxPatrol VM позволит:

- построить процесс, который будет работать
- контролировать уязвимости и повысить защищенность компании от реальных угроз
- оперативно выявлять критические состояния и быстро реагировать

MaxPatrol VM

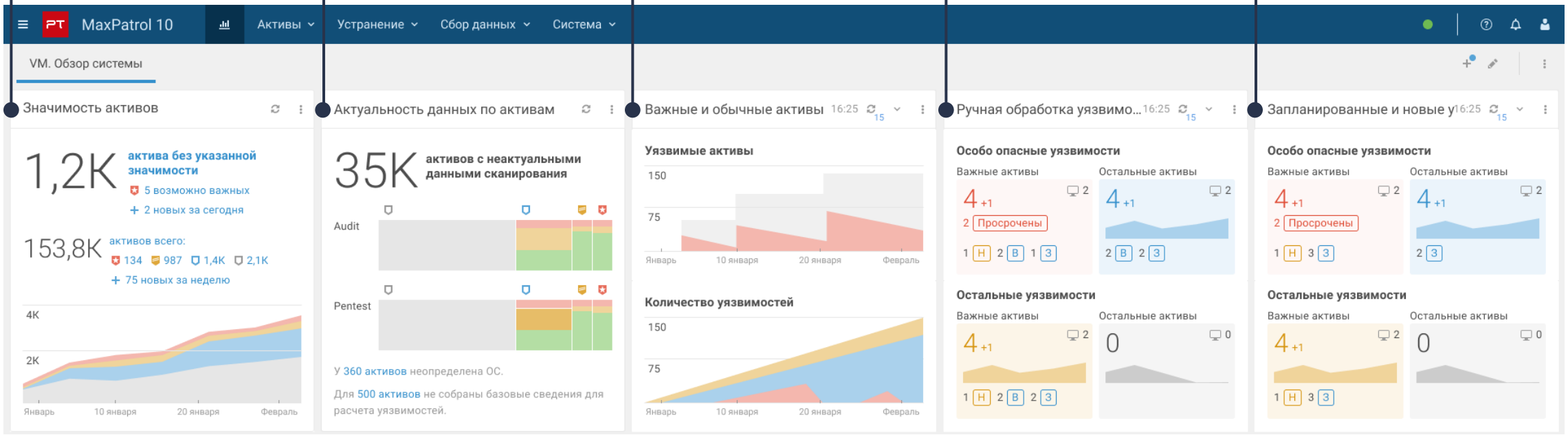
Нашли все активы в сети. Приоритизируй, чтобы знать, что важно

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

Контролируй, что происходит на важных активах. Отслеживай новые

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

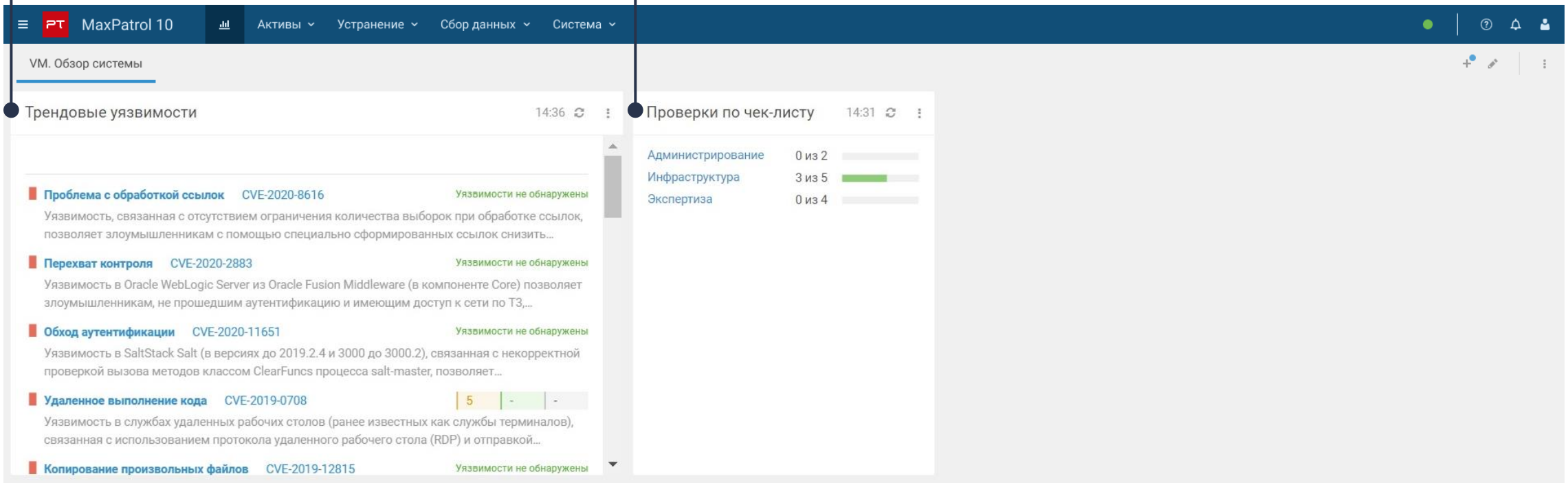
… и за нарушением SLA! Контролируй своевременное устранение



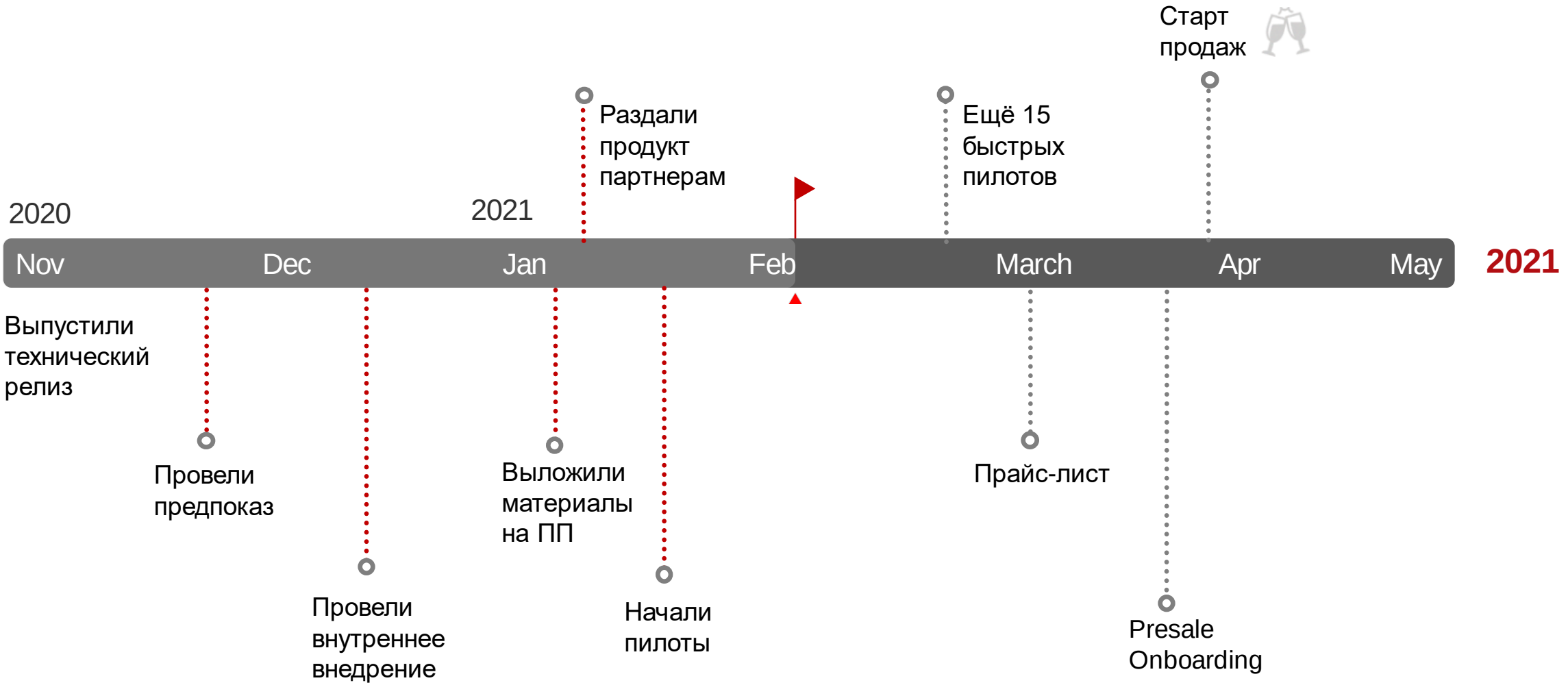
MaxPatrol VM

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

Следи за состоянием
внедрения VM



Что дальше?


Старт продаж
Раздали продукт партнерам
Ещё 15 быстрых пилотов
2020
2021
Nov
Dec
Jan
Feb
March
Apr
May
2021
Выпустили технический релиз
Провели предпоказ
Провели внутреннее внедрение
Выложили материалы на ПП
Начали пилоты
Прайс-лист
Presale Onboarding

Нам нужны пилоты

сколько и какие

ptsecurity.com

Совместные пилоты

Сроки

до конца марта

Объем инфраструктуры

До 2000 узлов

Тип заказчика

- Лояльный заказчик
- Нет VM-продукта или есть наш MP 8/ MP SIEM
- Ему **не всё равно** на безопасность
- Он хочет разобраться с управлением уязвимостями

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

О чем говорить

до и после пилота

ptsecurity.com

О чем мы говорим с заказчиком?

Вопрос №1:	Как вы собираете данные об инфраструктуре?
Вопрос №2:	Как вы реагируете на выявленные уязвимости?
Вопрос №3:	Как вы договариваетесь с IT-отделом?
Вопрос №4:	Как вы оцениваете уровень защищенности компании?

Что мы уже слышали?

Ваш VM похож на SIEM!

У меня уже есть процесс и он другой!

Мы не можем закрывать уязвимости на всех системах.

Мне нужна интеграция с тикет-системой для экспорта уязвимостей в IT!

Мне нужен функционал X.

У меня уже всё работает с MaxPatrol 8!

Спасибо

ptsecurity.com