

# MaxPatrol SIEM 2.0

**Алексей Горелышев**

зам. директора Центра компетенции  
Positive Technologies

**POSITIVE TECHNOLOGIES**

[ptsecurity.com](https://ptsecurity.com)

# MaxPatrol SIEM:

итоги первого года на рынке РФ



**51**

**Пилотный  
проект**



**26**

проектов  
завершено



**25**

проектов  
в процессе

**Коммерческие  
результаты**

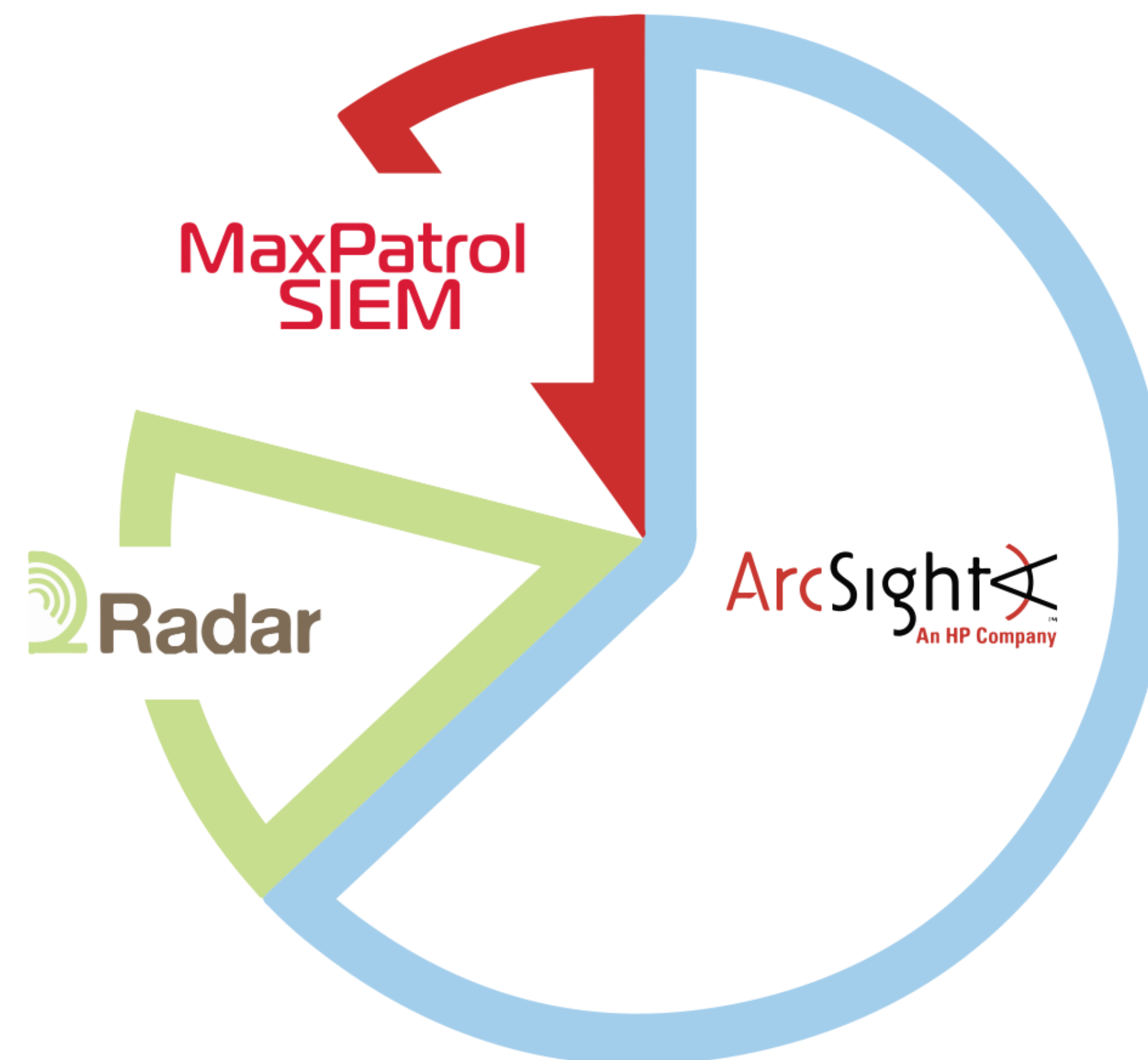
**180 Р  
млн ₴**

продажи  
MaxPatrol SIEM

**15** коммерческих  
проектов

**10%** Российского  
рынка

За первый год продаж MaxPatrol SIEM  
добился видимых результатов  
и завоевал более 10% российского рынка





## Заказчики MaxPatrol SIEM



ДИТ

ДИТ Москвы



РОССЕТИ

Россети



КиС СПб



Министерство  
транспорта



Министерство обороны

## Прогноз 2016

60+

ПИЛОТОВ

35+

коммерческих  
проектов

500  
млн **₽**

продажи  
MaxPatrol  
SIEM



## MaxPatrol SIEM

- ❑ Научились хорошо делать пилотные проекты (4/5)
- ❑ Поставили процесс поддержки источников «по требованию»
- ❑ Предсказуемая разработка продукта и понятный roadmap
- ❑ Сертификация (МинОбороны, ФСТЭК) и соответствие российским стандартам
- ❑ С нами наши Партнеры
- ❑ С нами наши Заказчики
- ❑ Решение работает и быстро прогрессирует





# MaxPatrol SIEM 2.0



## SIEM

**СБОР**

**КОРРЕЛЯЦИЯ**

**ИНЦИДЕНТЫ**

Нормализация  
Фильтрация  
Агрегация  
Хранение  
Отображение  
Отчётность  
Уведомления







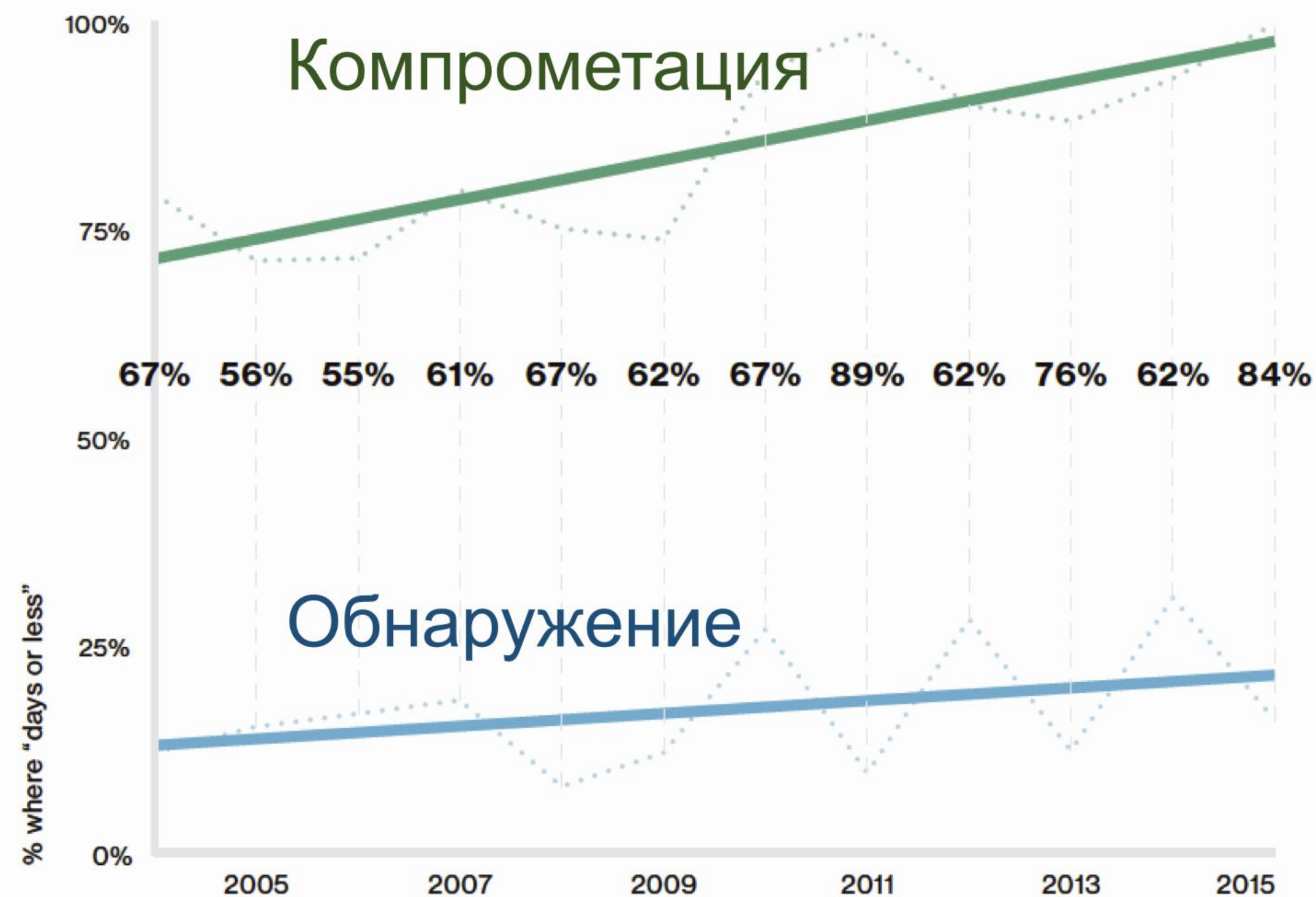
## Часы, минуты

занимает компрометация



## Недели, месяцы

проходят до обнаружения



## В чём проблема?

Сложность внедрения  
и сопровождения

Высокая чувствительность  
к инфраструктуре

Необходимость  
множества решений

Каждый заказчик  
должен стать экспертом!

## Должно быть

Легко и удобно

Адаптируется к изменениям

Единая платформа

Готовая экспертиза



**MaxPatrol**  
Vulnerability Management

**MaxPatrol**  
Threat Modeling

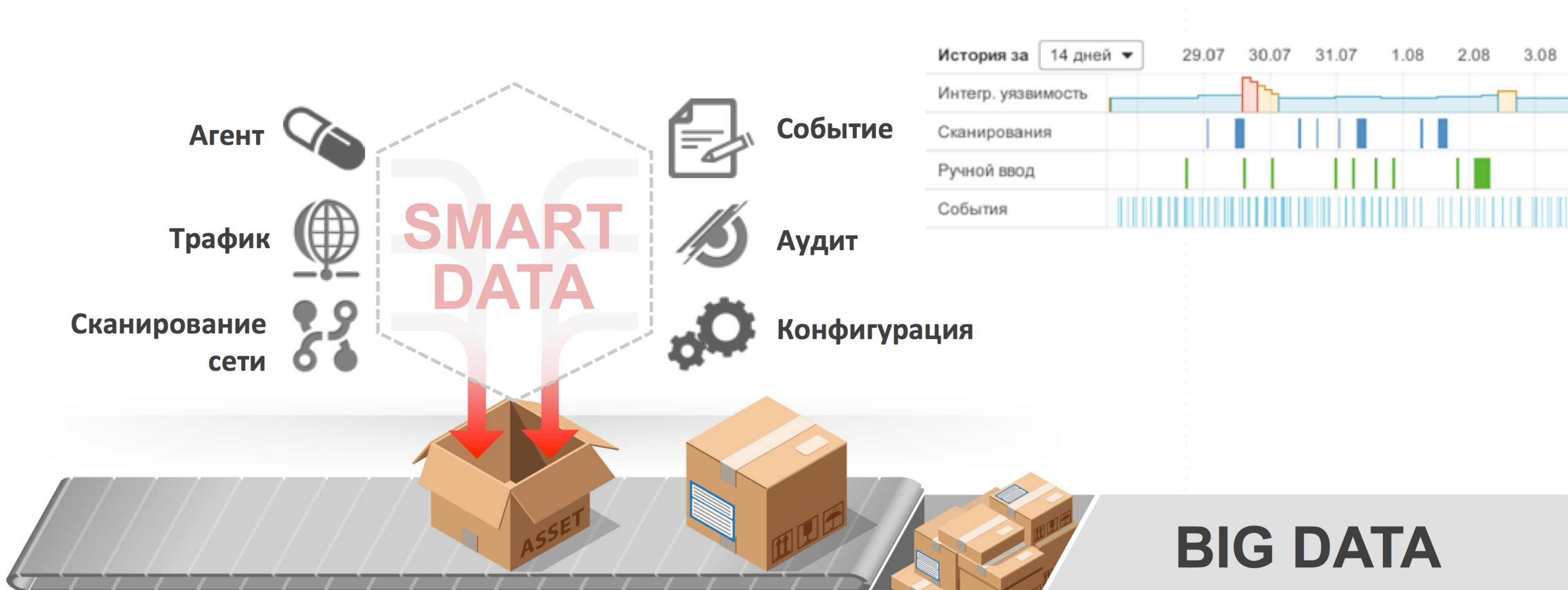
POSITIVE TECHNOLOGIES  
**MaxPatrol**  
**SIEM**

**MaxPatrol**  
Platform

**MaxPatrol**  
Host Compliance & Control

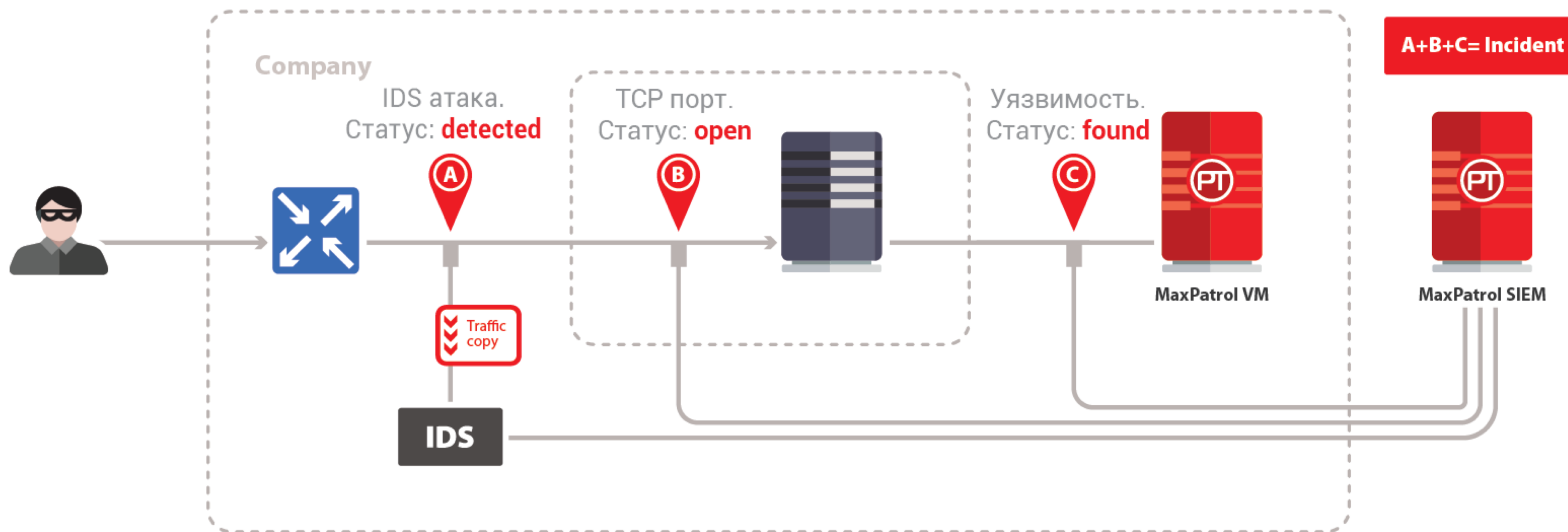
**MaxPatrol**  
Network Compliance & Control

**MaxPatrol**  
Network Storage & Forensic















— 100 —

— 200 —

— 500 —



1

Актив  
во времени

2

Модельные  
корреляции

3

Новый интерфейс

4

Множественная  
сортировка

5

Управления правилами  
корреляции

6

Простой поиск

7

Управление  
инцидентами

8

Новые  
отчёты

9

Уведомления

**MaxPatrol**  
Vulnerability Management

**MaxPatrol**  
Threat Modeling

POSITIVE TECHNOLOGIES

**MaxPatrol**  
**SIEM**

**MaxPatrol**  
Platform

**MaxPatrol**  
Host Compliance & Control

**MaxPatrol**  
Network Compliance & Control

**MaxPatrol**  
Network Storage & Forensic

**ЭКСПЕРТИЗА**





# MaxPatrol SIEM Roadmap 2016



## R12 (SIEM 2.0)

Апрель

### Release Concept

Поддержка управления правилами корреляций в UI интерфейсе

Быстрый поиск и фильтрация активов по ключевым полям(IP, FQDN, Hostname)

Модельные корреляции

Фильтры по инцидентам, email уведомления по инцидентам

Расширенные возможности по работе с событиями

## R13

Июль

### Release Concept

Облачное обновление данных по уязвимостям

Развитие функционала динамических групп (скорость, описание, расширение полей, контекст)

Расширение возможностей в механизме расписаний сканирования, генерации отчетов,

Улучшение возможностей в работе с топологией сети

## R14

Сентябрь

### Release Concept

Глубоко настраиваемая отчетность

EndPoint движок

Расчет сетевой достижимости L3

Конструктор формул нормализации

SIEM на стороне агента

## R15

Декабрь

### Release Concept

Автоматическая генерация правил корреляции на основе векторов атак на базе движка достижимости

Пользовательские модули обработки событий

Централизованное управление иерархической инсталляцией

Упрощённый генератор формул корреляций

POC: работа всех сервисов на Linux

# Спасибо

POSITIVE TECHNOLOGIES

[ptsecurity.com](https://ptsecurity.com)