MaxPatrol SIEM
Переосмысление SIEM

Максимович Максим

Отдел проектирование и внедрения
Positive Technologies

POSITIVE TECHNOLOGIES

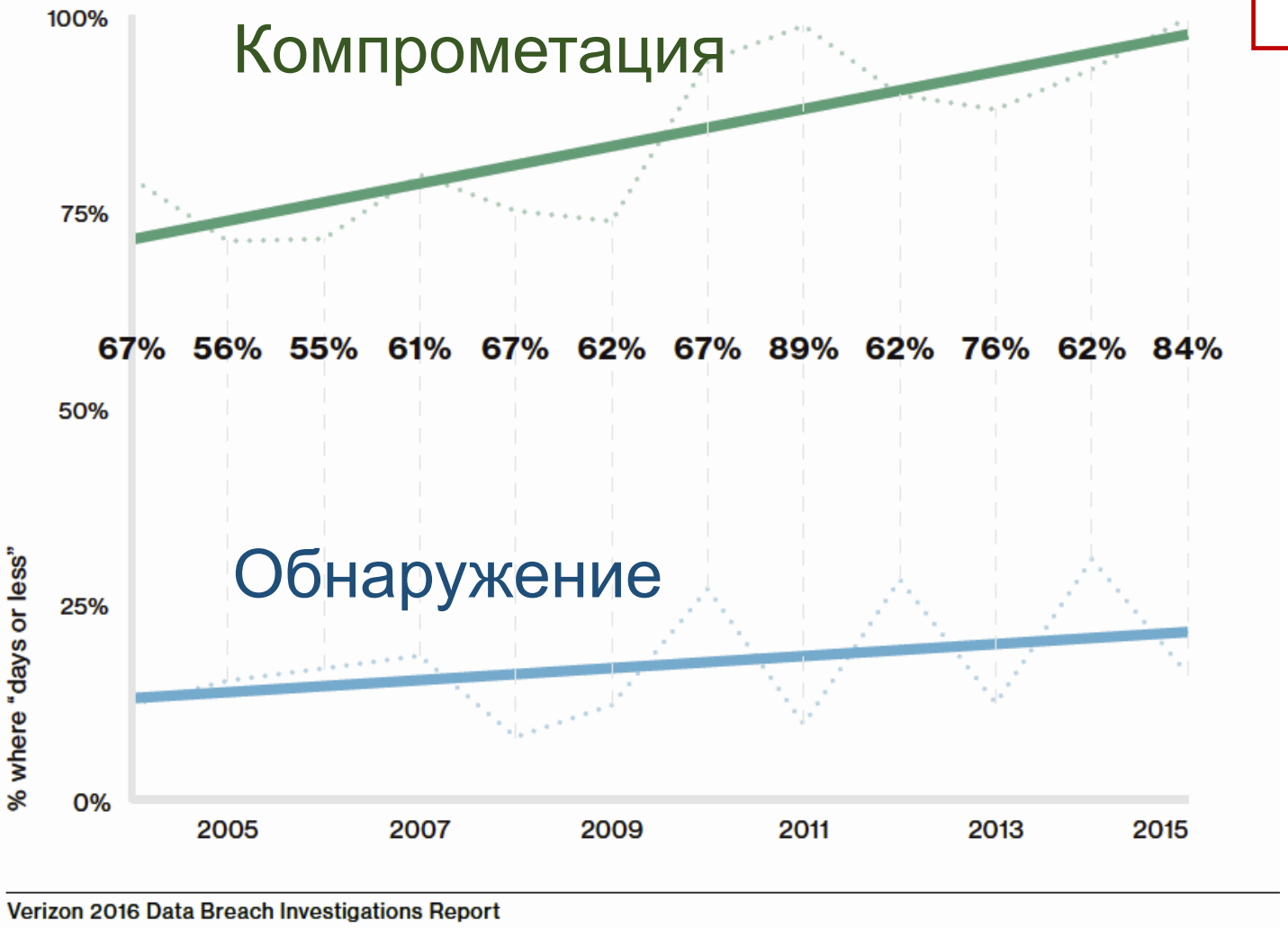
ptsecurity.com

Подходы
Тренды
Статистика

Почему-то всё равно не работает

Часы, минуты
занимает
компрометация

Недели, месяцы
проходят до
обнаружения



Verizon 2016 Data Breach Investigations Report

Тесты на проникновение

87%

Периметр 87% корпоративных локальных сетей не останавливает проникновение

61%

61% может взломать неквалифициро-ванный хакер

1 неделя

Взлом ЛВС компании занимает 3-5 дней

2%

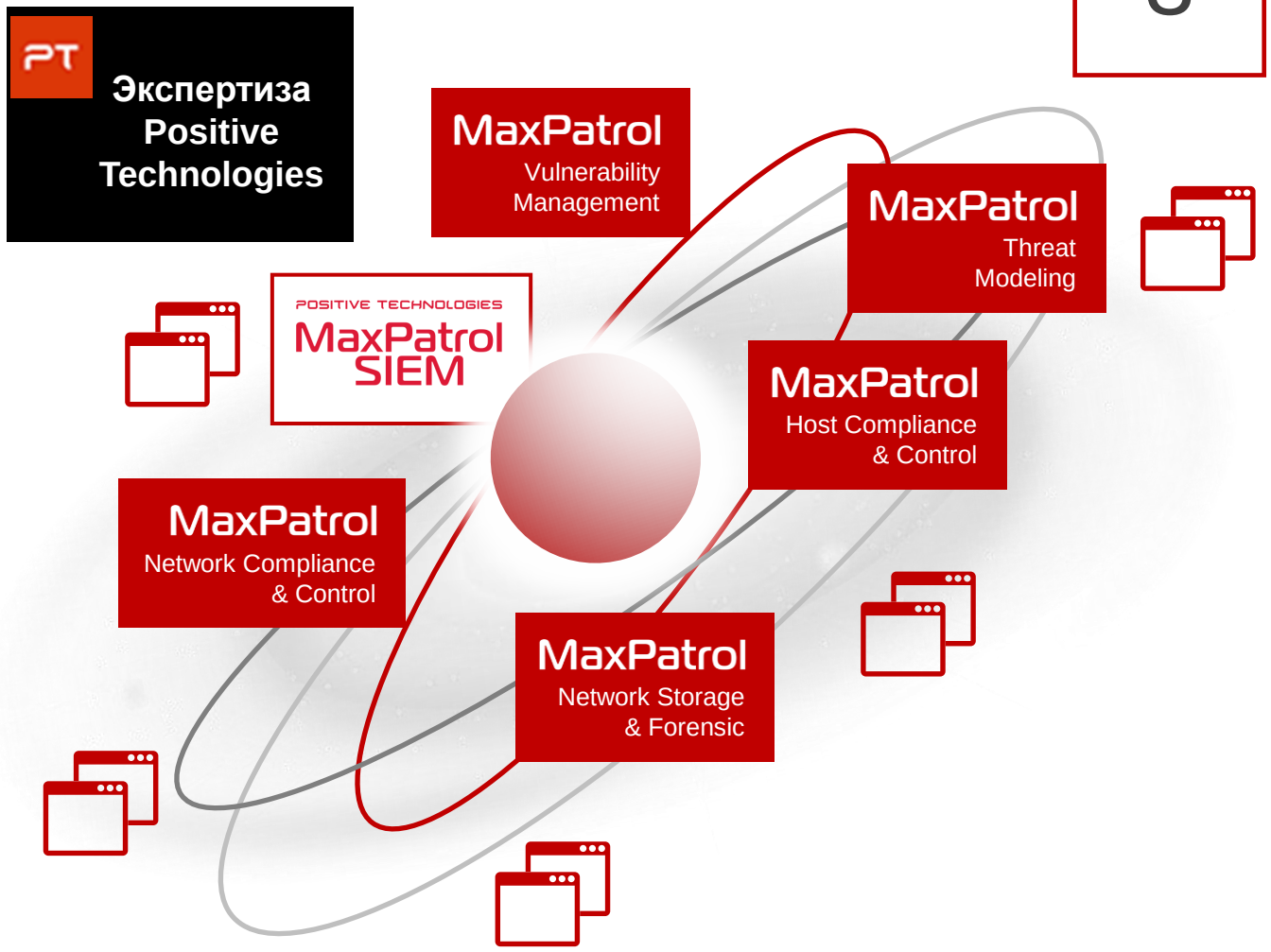
Действия пентестеров обнаруживаются только в 2% тестов на проникновение

Одна цель – множество систем – одна платформа

- 13 лет масштабных тестов на проникновение
- Сотни найденных 0-day уязвимостей в год
- Ежедневные анализы реальных инциденты ИБ
- Positive Expert Security Center – всегда на переднем крае
- Аналитика и моделирование атак
- Прототипирование и испытание технологий

MAXPATROL

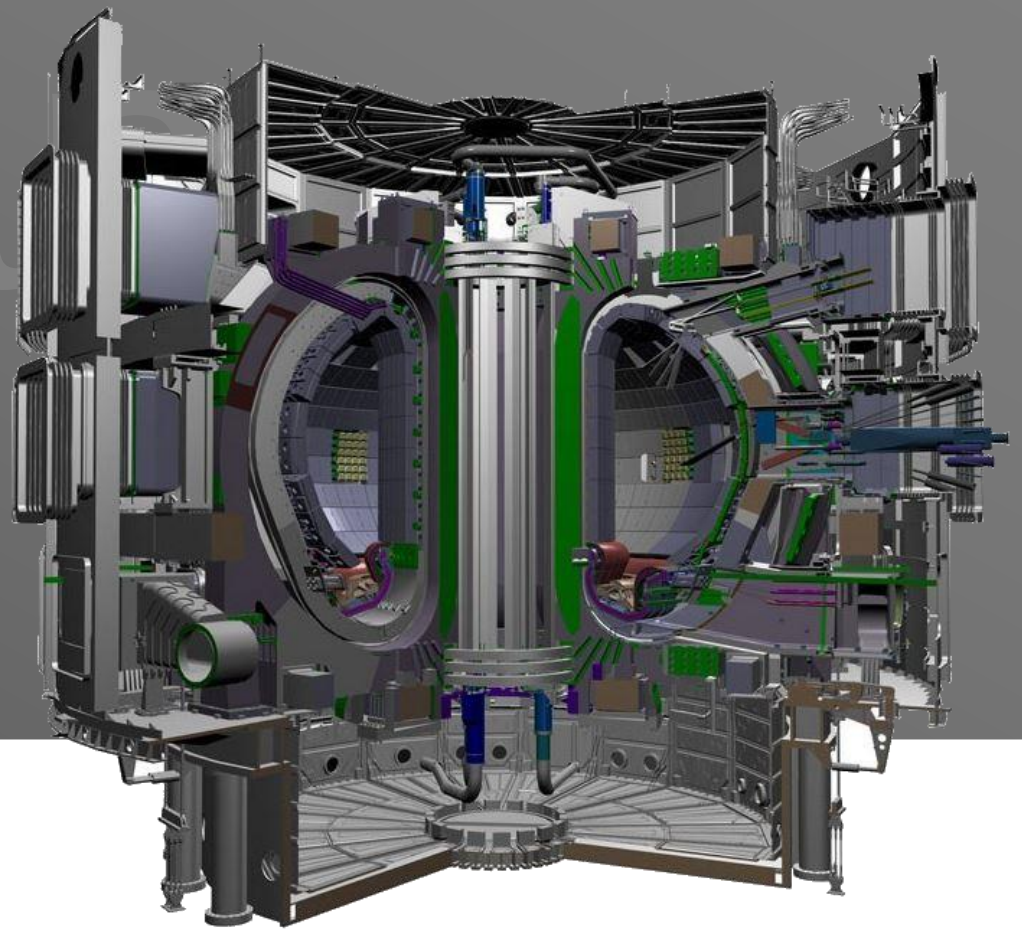
уникальная платформа объединяющая в себе множество направлений



MaxPatrol SIEM

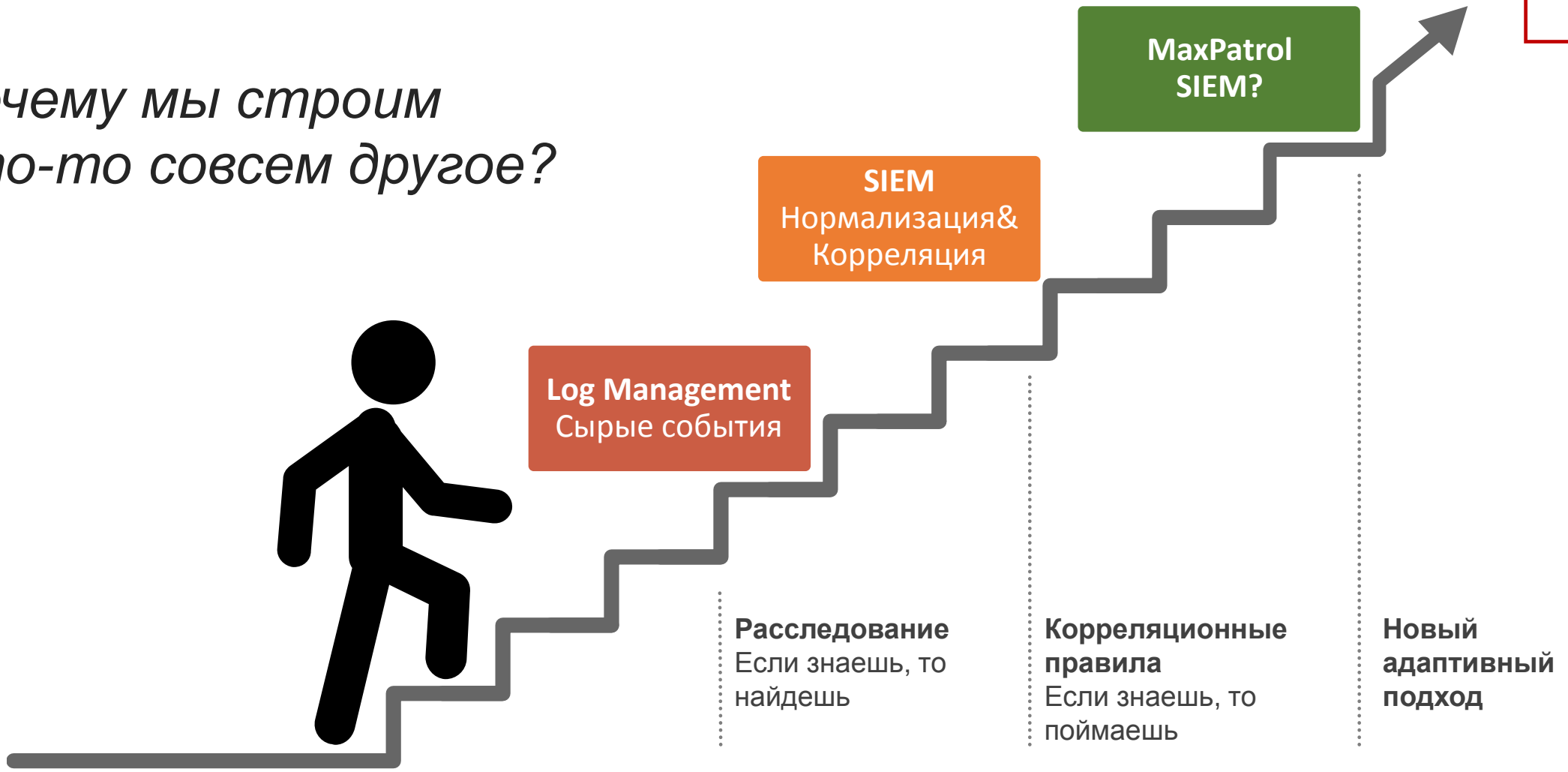
More than SIEM

Переосмысление SIEM

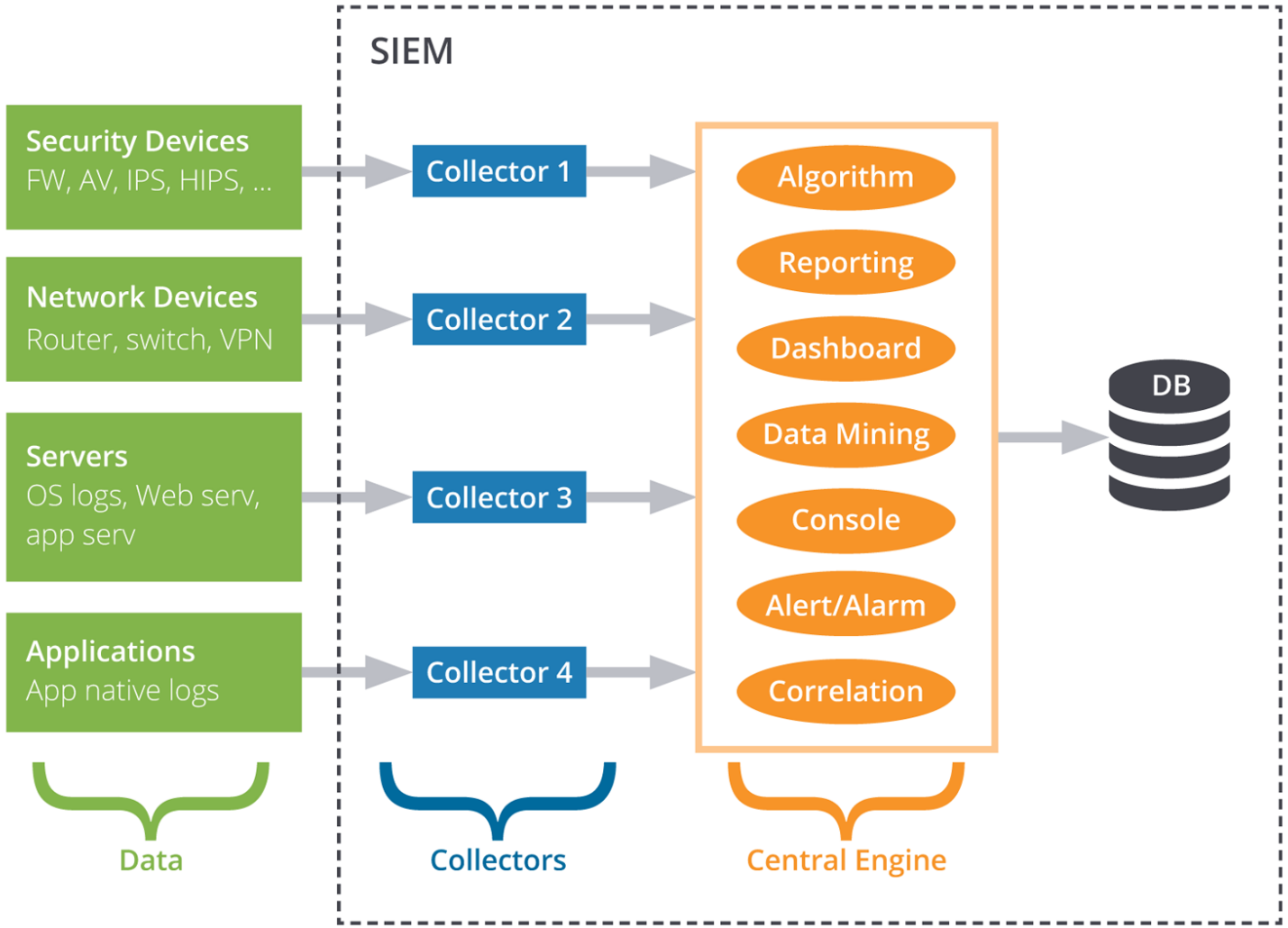


Почему MaxPatrol SIEM является другим решением?

Почему мы строим что-то совсем другое?



Классический SIEM: события с разных источников

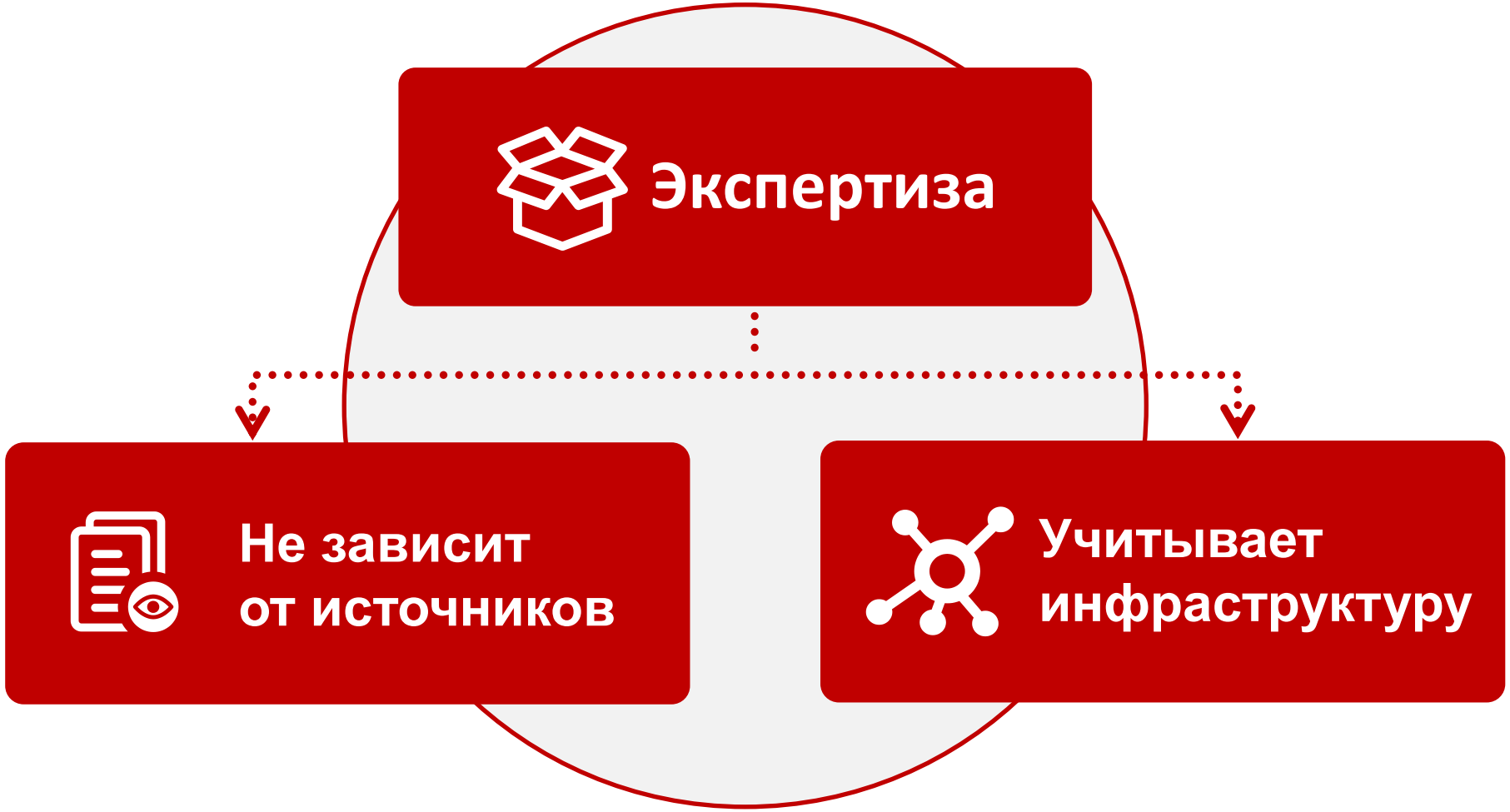


Классический SIEM(развитие): события + контекст

Расширенный контекст

Дополнительно к функции нормализации и корреляции событий на потоке SIEM оперирует информацией из внешних систем сбора конфигураций, анализа уязвимостей, white/black списков и выполняет более глубокую аналитику – тем самым обеспечивает более точную приоритезацию инцидентов, понижает уровень false-позитивов и позволяет выполнять более глубокую аналитику

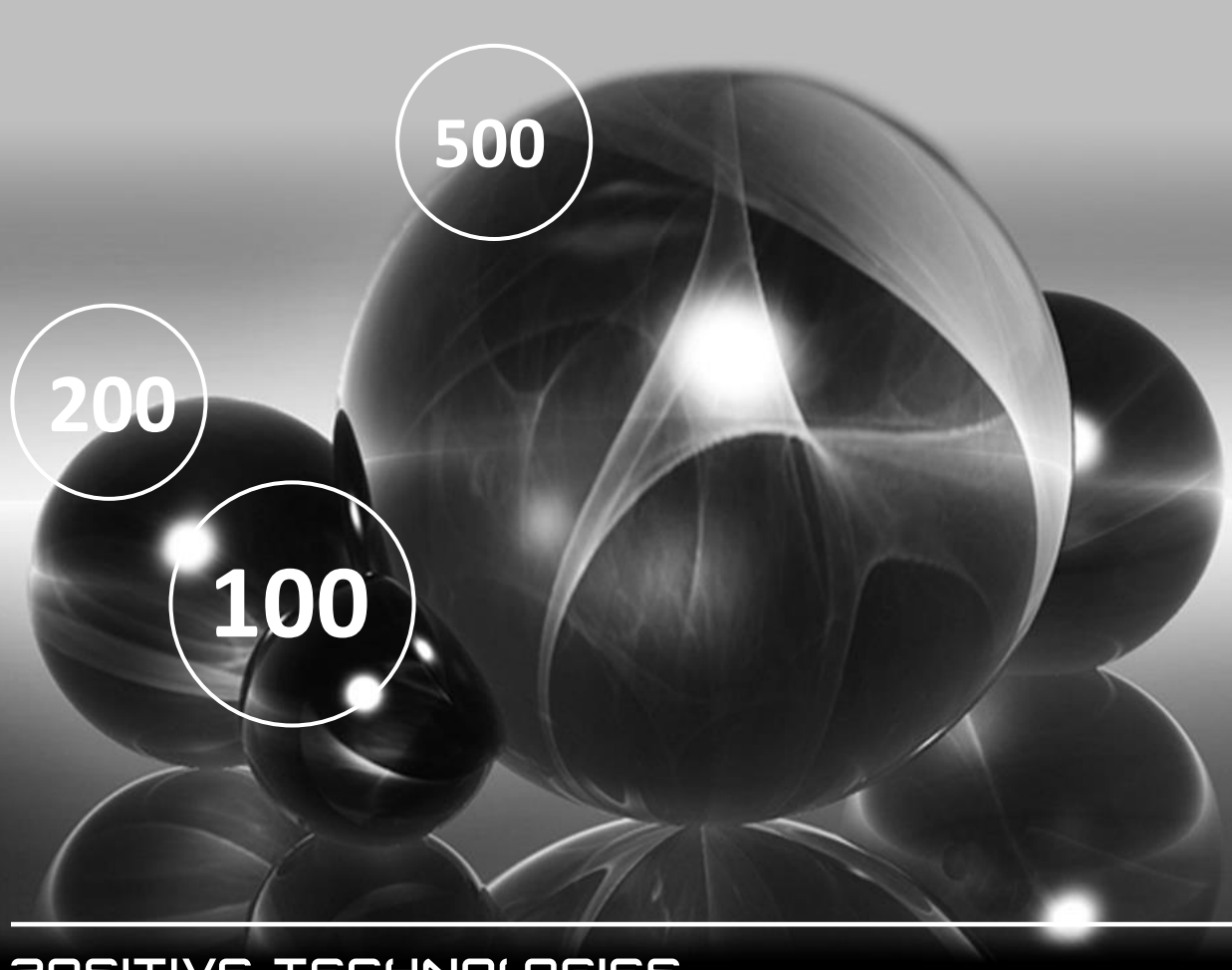
Экспертиза, которая должна работать из коробки!



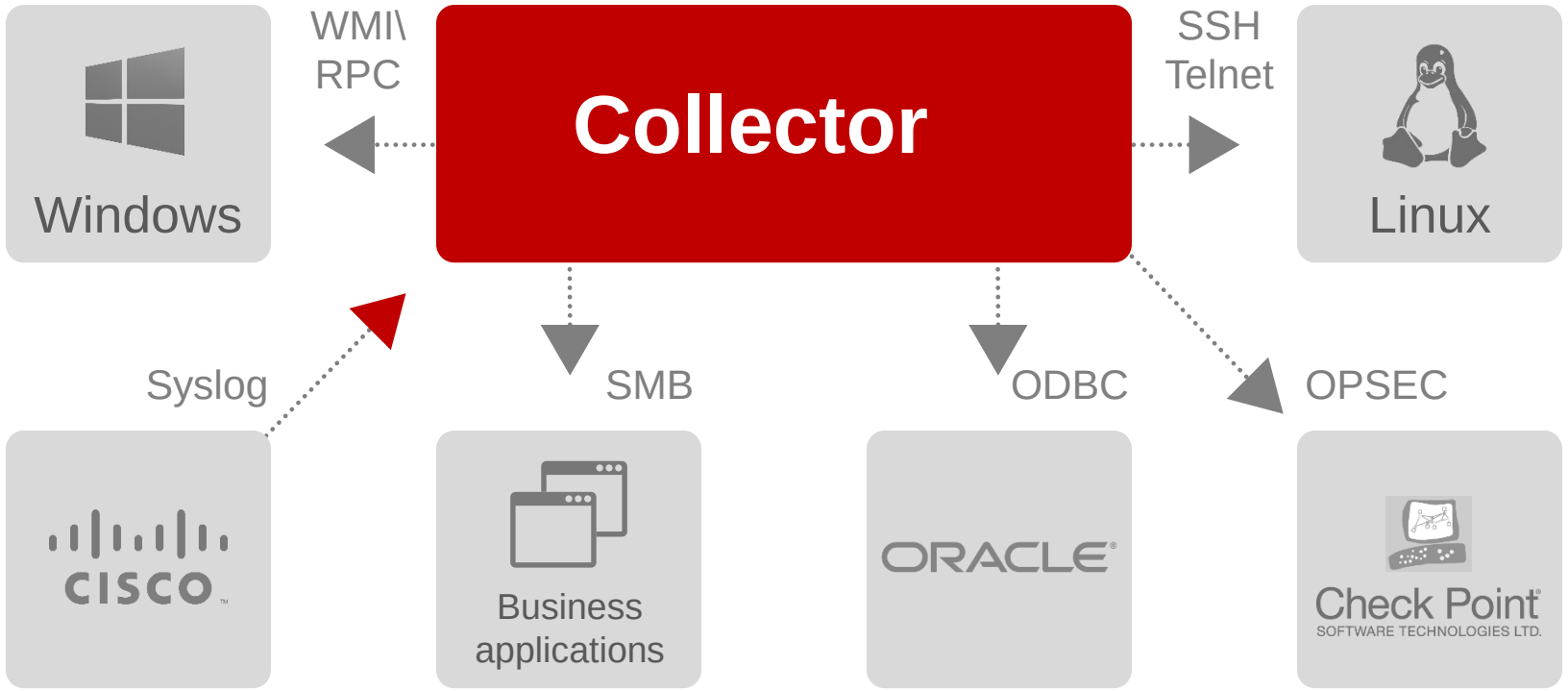
FREEDOM FROM DATA SOURCE ADDICTION

Сбор событий и обработка

У вас есть источник? Мы поддержим его из коробки!



Сбор



Пример:

Type: ODBC Oracle
Port: 1521
Instance: ORCL
Query:

```
select
    id, date, user, action, host
from (select ….
where
    action = “denied”
order by …
```

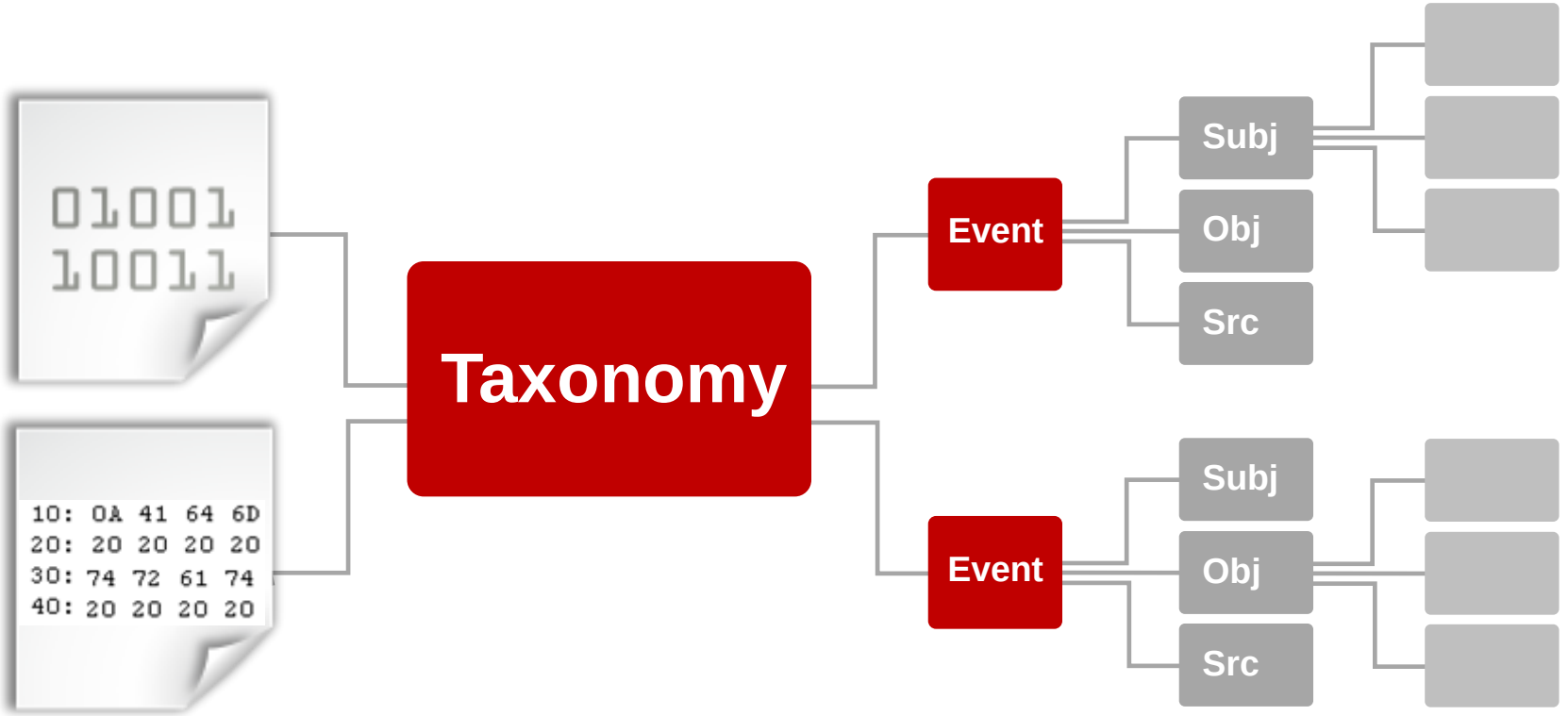
Interval: 1000
…

Taxonomy and normalization unification

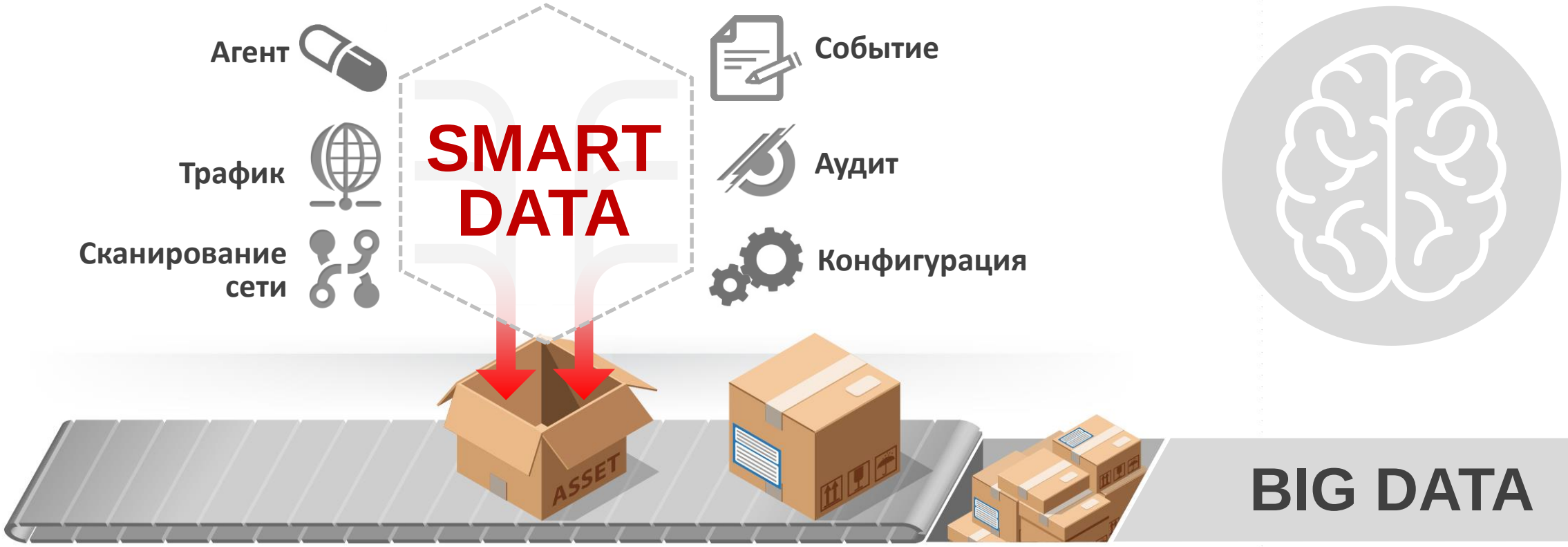
Сотни не зависящих друг от друга полей VS **70** структурированных объектно-ориентированных полей в MaxPatrol SIEM!

Получить правила, работающие из коробки

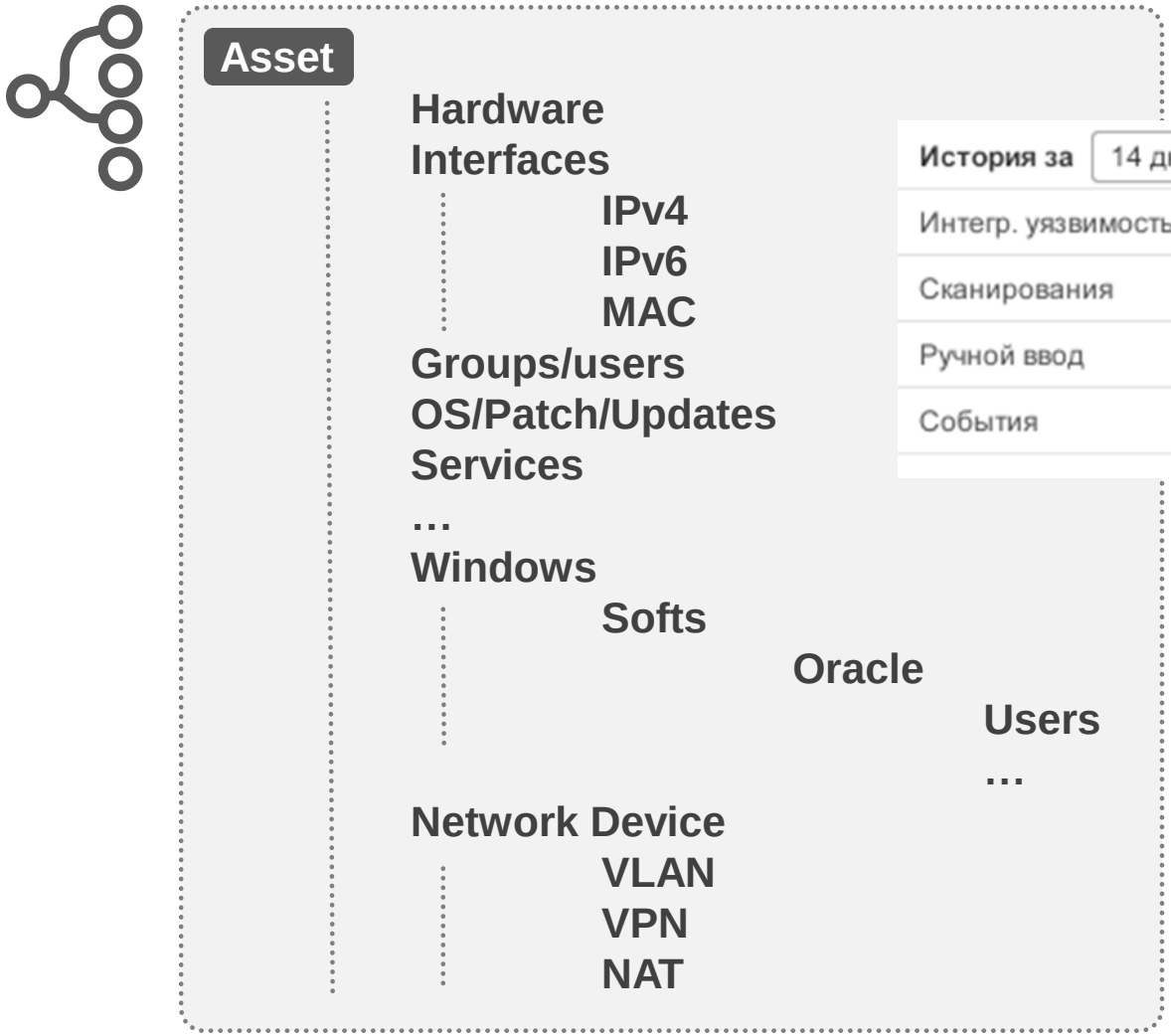
Свести шансы на ошибку в процессе нормализации до нуля

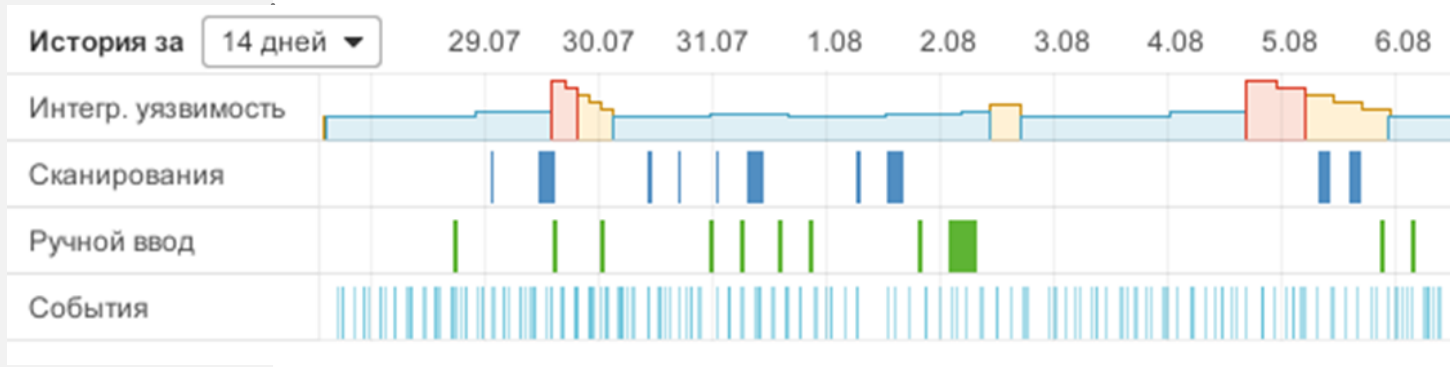


Активо-центрический подход

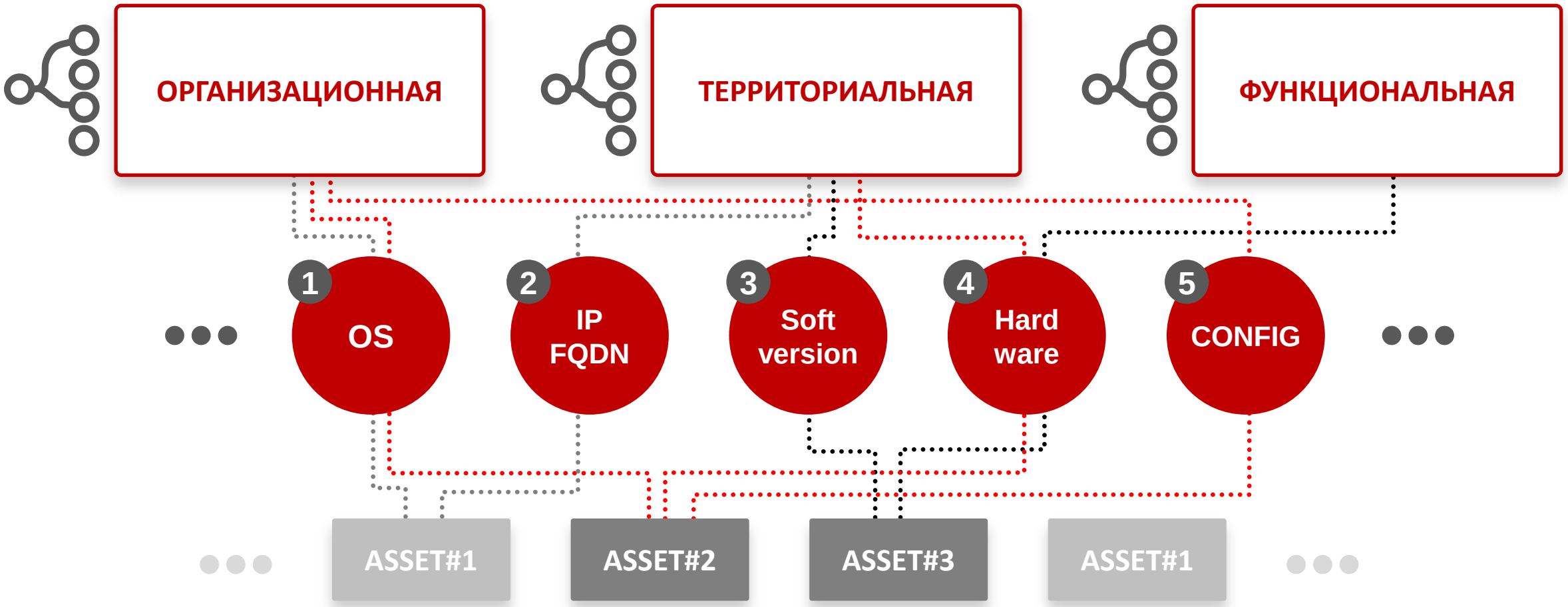


Метамодель актива





Управление активами



Уже сегодня – модельные корреляции

POSITIVE TECHNOLOGIES

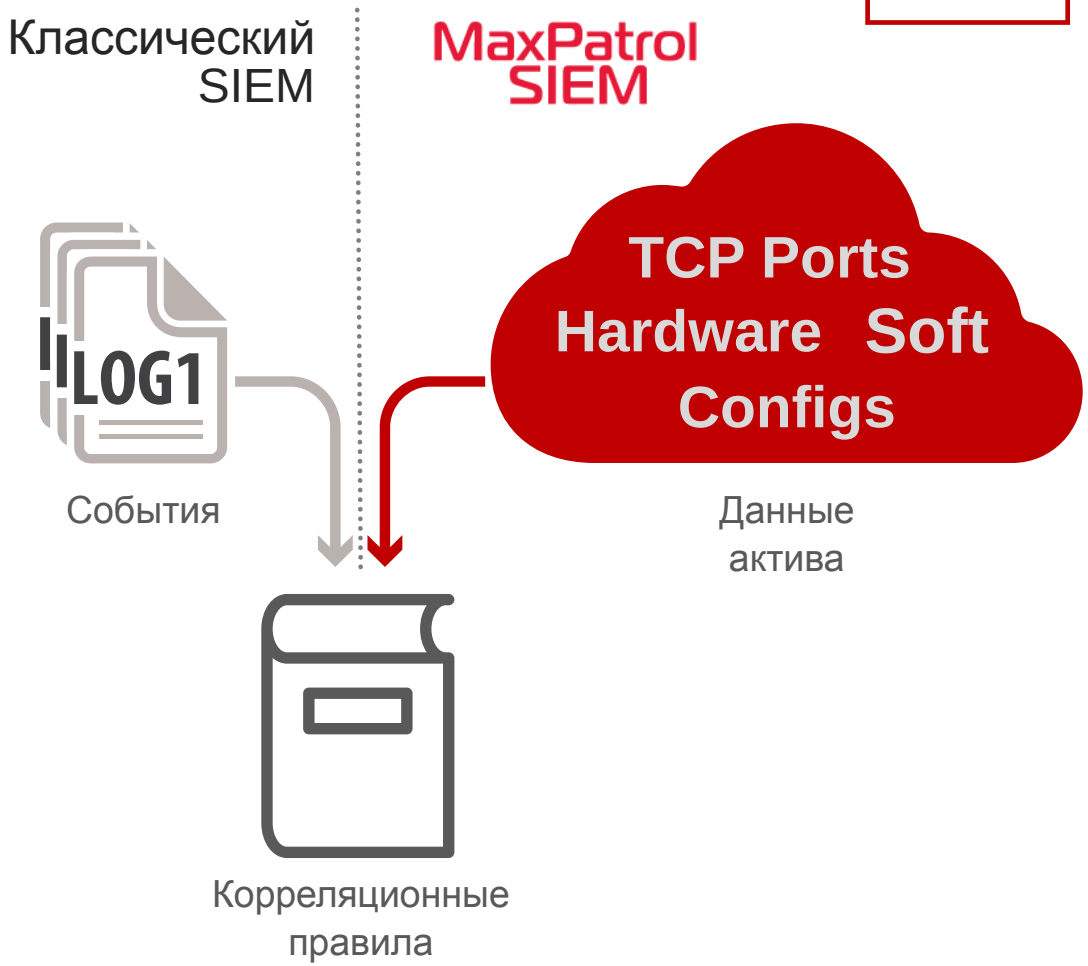
ptsecurity.com

Модельные корреляции

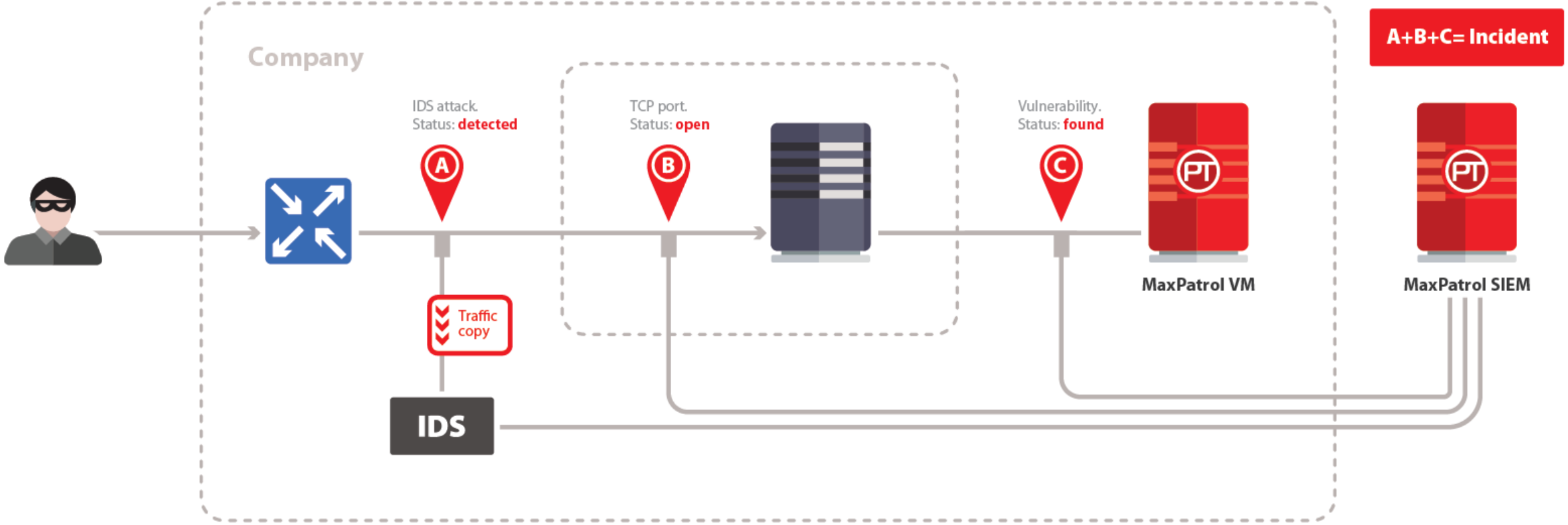
3 **query Q**(ip, port) from endpoints
    Group = "DMZ" and Endpoints(Address= ip
    and Port = port and Status = "Open")

2 **event E**
        key: dst.ip
        filter *object* = "attack" and
        category = "IDS/IPS" and
        query.Q(dst.ip, dst.port)

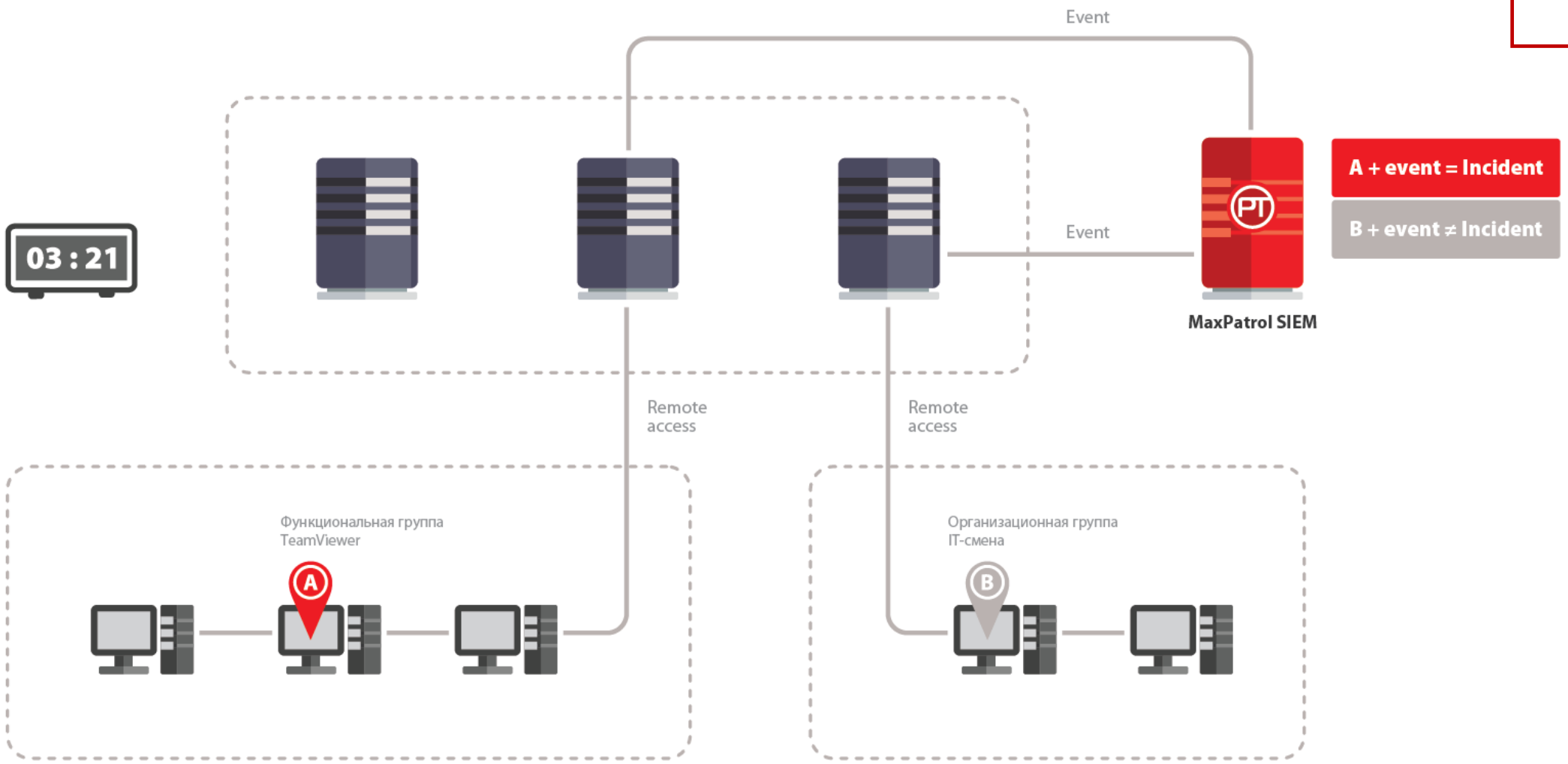
1 **rule** *DMZ_host_attack*: Event.E[5] within 1 day



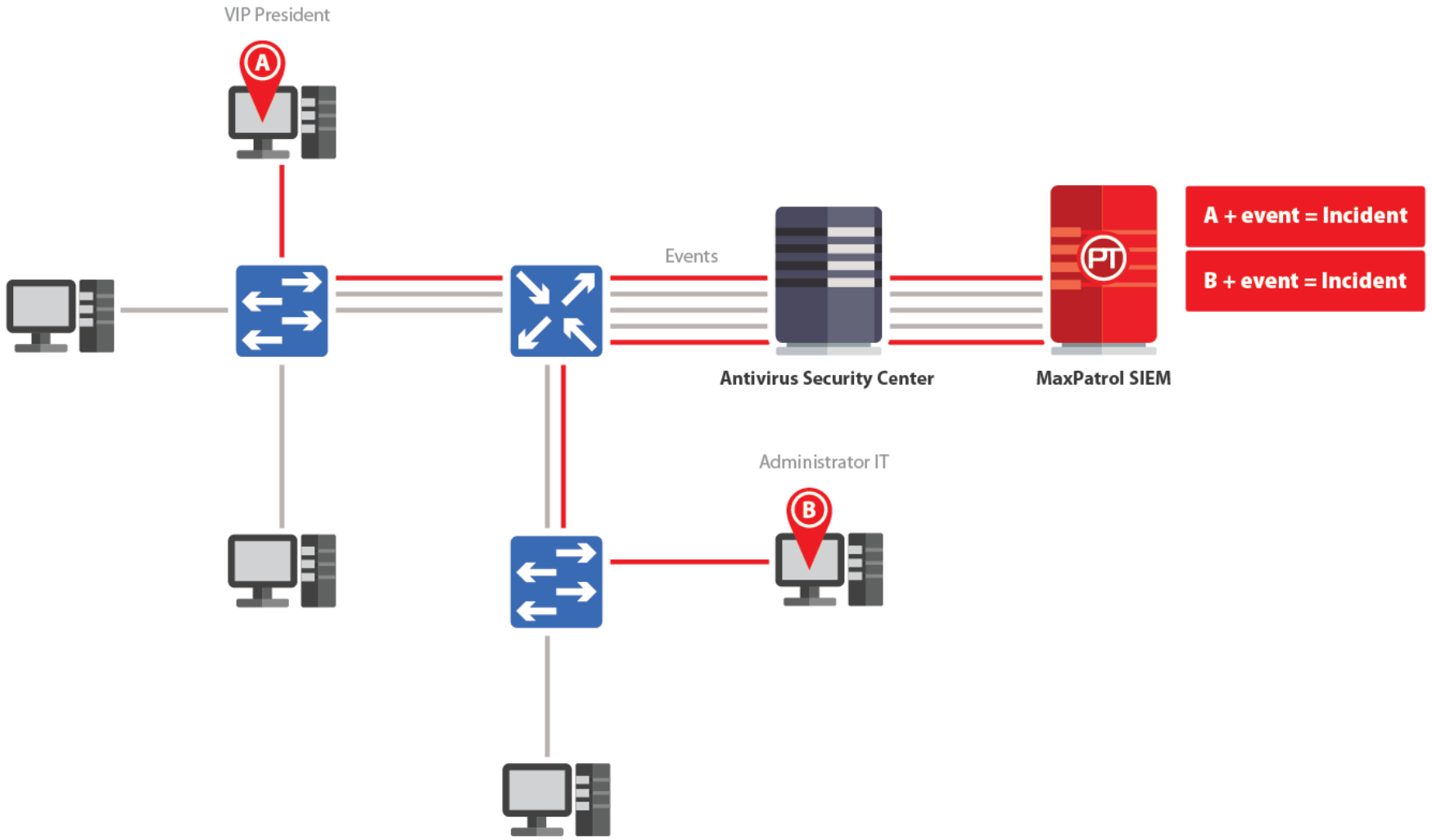
Пример модельной корреляции №1



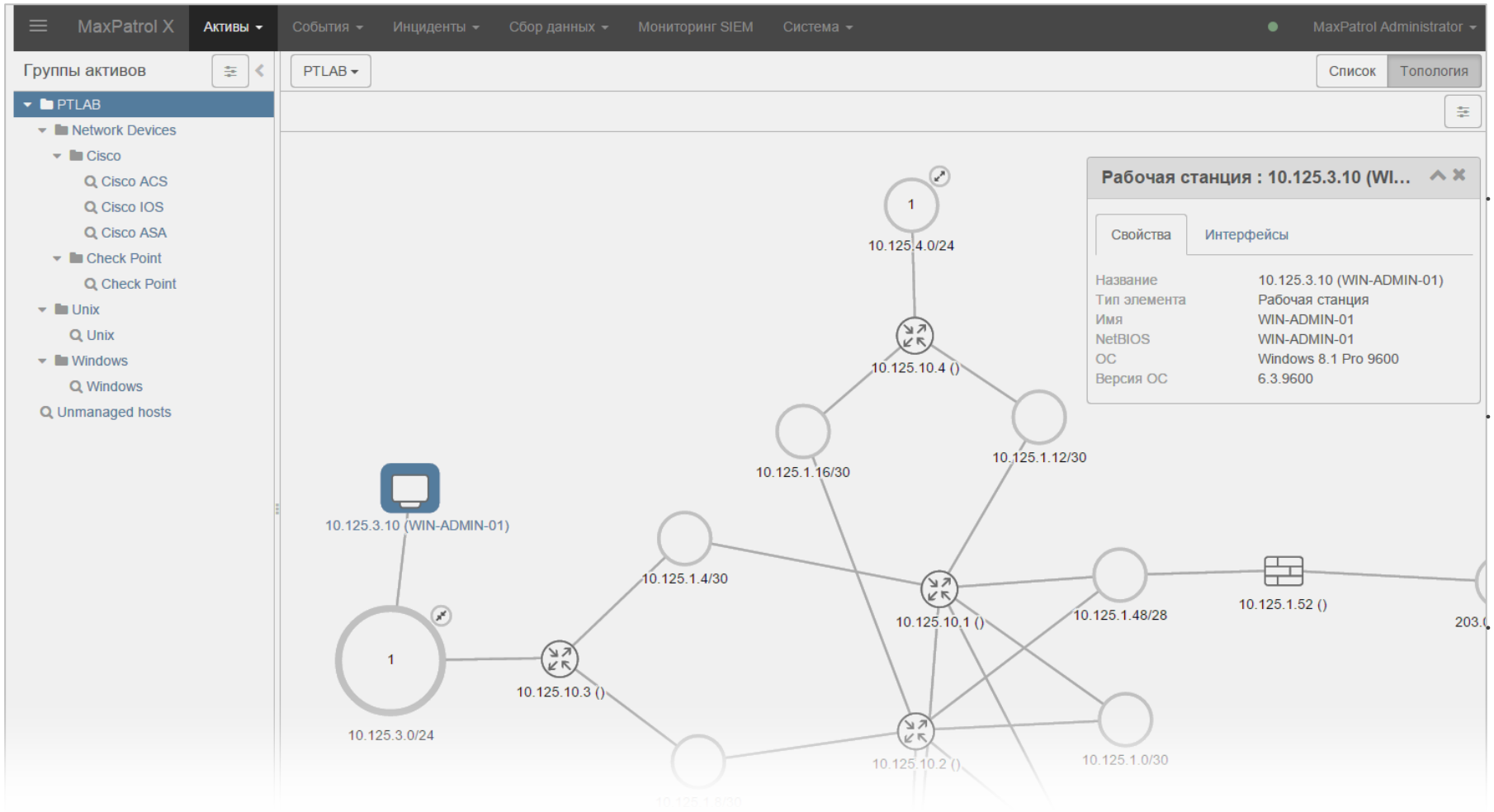
Пример модельной корреляции №2



Пример модельной корреляции №3



Топология – достижимость – вектора атак



1

2

3

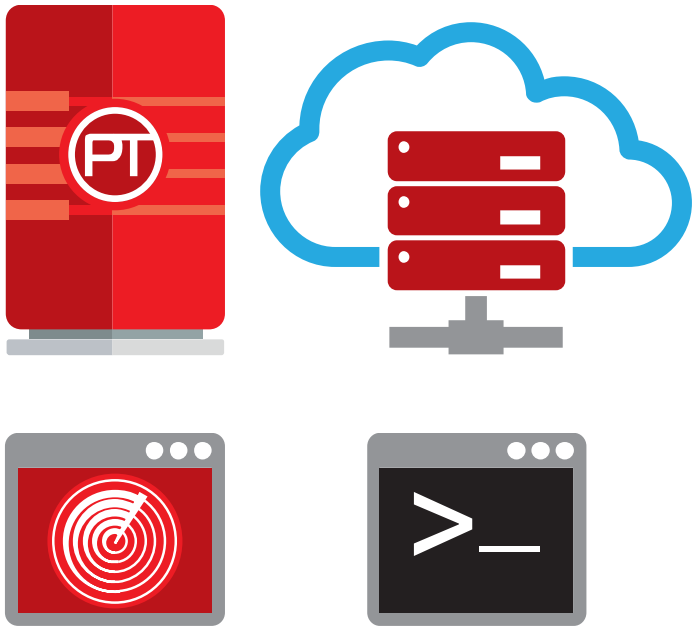
MaxPatrol SIEM. Архитектура

POSITIVE TECHNOLOGIES

ptsecurity.com

Компоненты

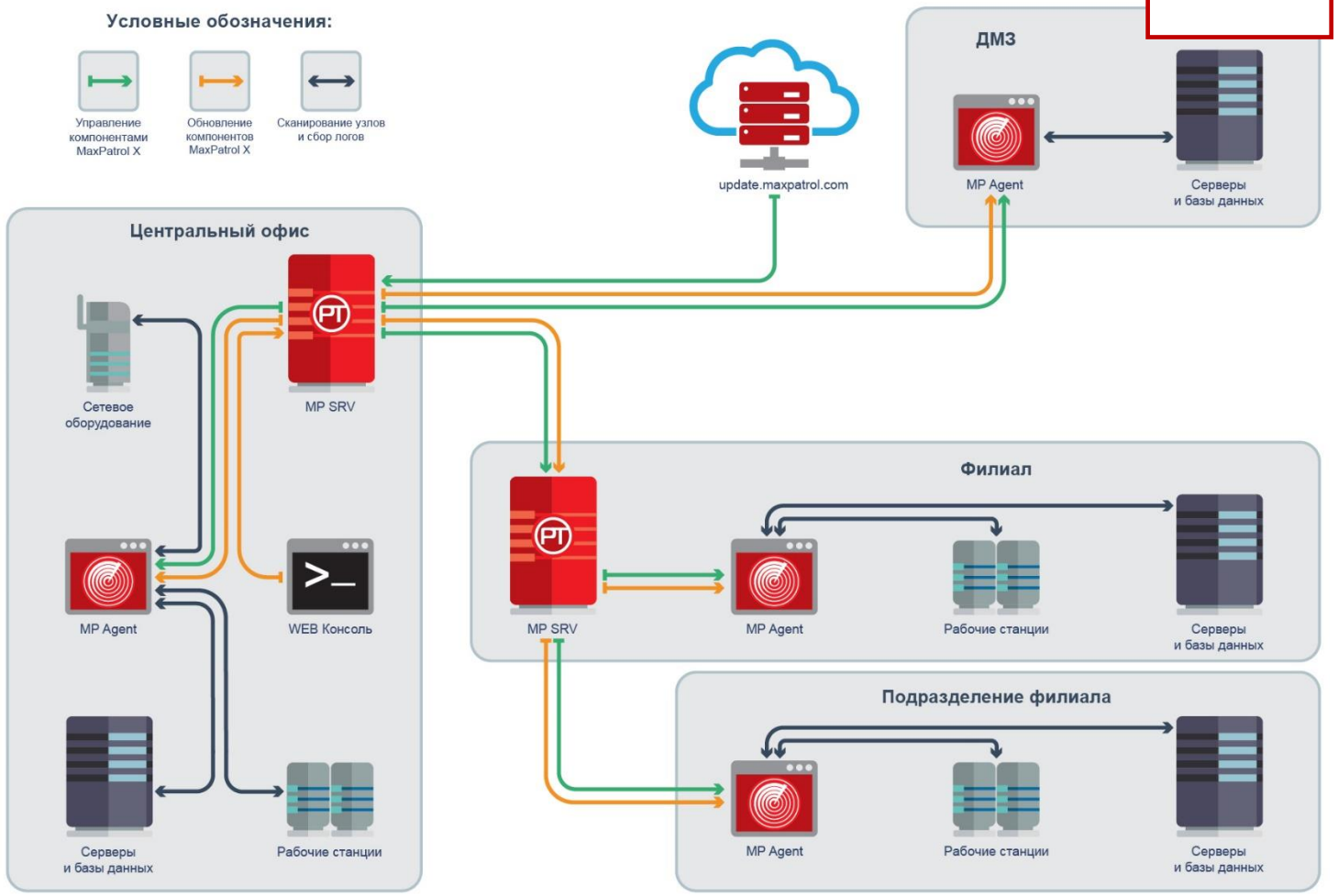
POSITIVE TECHNOLOGIES
MaxPatrol SIEM



- MaxPatrol Server
- MaxPatrol Scanner
- MaxPatrol Log Collector
- MaxPatrol Network Traffic
- MaxPatrol Host Control

Платформа MaxPatrol: Архитектура

- Масштабирование с учетом инфраструктуры клиента
- Оптимизация передачи данных по слабым каналам
- Увеличение производительности и объемов хранимых данных без дополнительных лицензий
- Удобство развертывания компонентов
- Встроенные механизмы диагностики
- Программы обучения персонала
- Оперативная техническая поддержка
- Возможность доработки производителем



Спасибо!

POSITIVE TECHNOLOGIES

ptsecurity.com