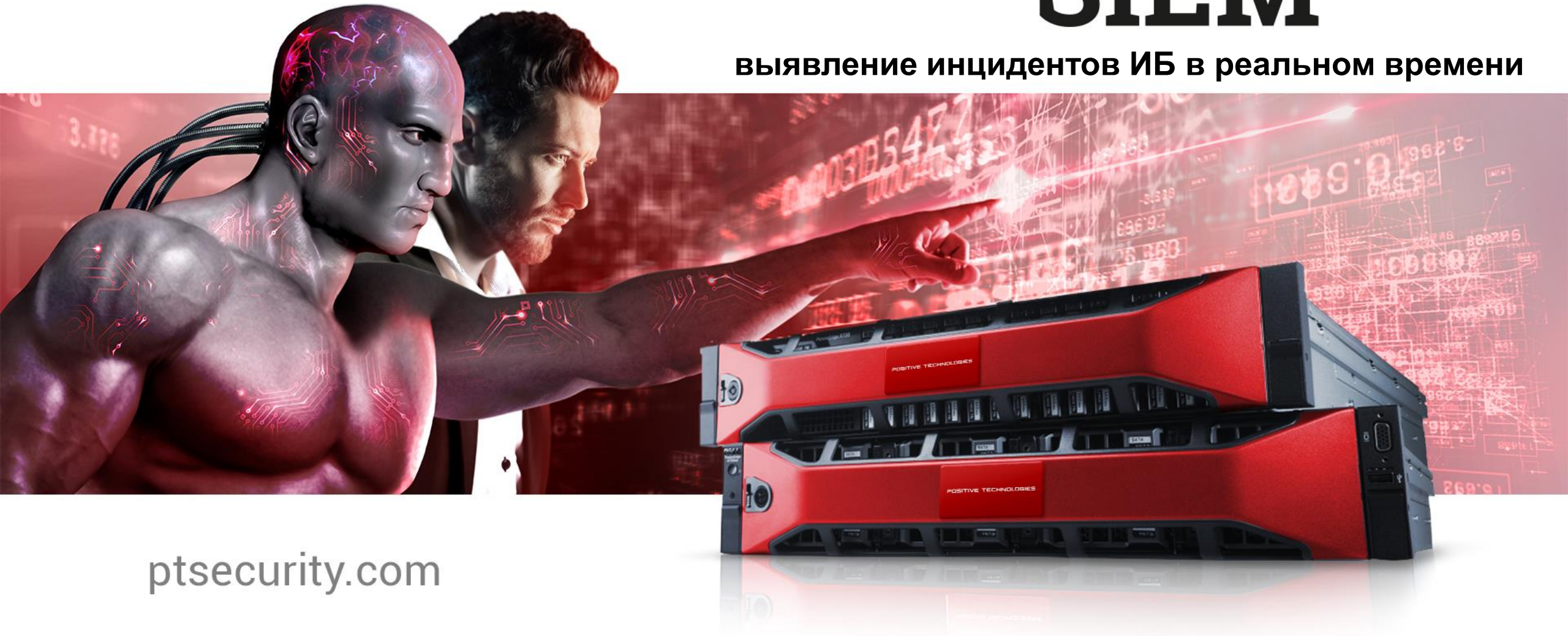
POSITIVE TECHNOLOGIES

MaxPatrol SIEM

выявление инцидентов ИБ в реальном времени



ptsecurity.com

Positive Technologies

в цифрах и фактах

О компании Positive Technologies

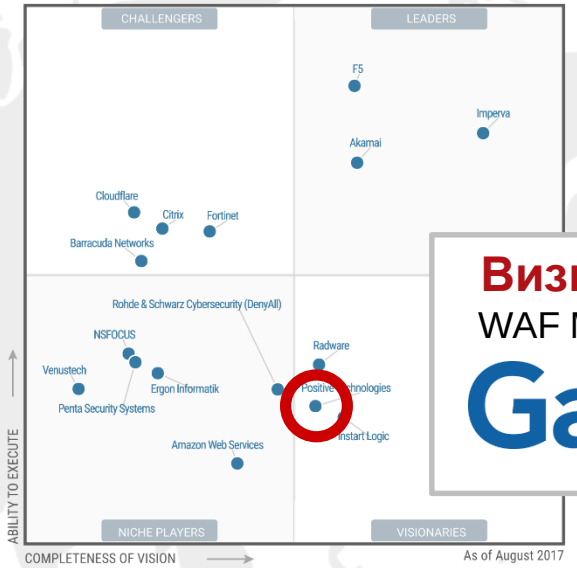
POSITIVE TECHNOLOGIES

200+
аудитов безопасности корпоративных систем

200+
обнаруженных уязвимостей нулевого дня

Главные продукты

- MaxPatrol
- MaxPatrol SIEM
- PT ISIM
- PT Application Firewall



Визионер 2017
WAF Magic Quadrant
Gartner®

15 **лет исследований и экспертизы**

150+ уязвимостей нулевого дня в системах SCADA

50+ расследований взломов инфраструктуры

500+ исследований безопасности мобильных и веб-приложений

История компании

POSITIVE TECHNOLOGIES

1999
Выход бесплатной open-source-версии **XSpider**

2000
Более **500 000** пользователей **XSpide**r по миру

2001
Открыт портал по безопасности **SecurityLab.ru**

2002
Основание компании **Positive Technologies**

2003
Выпуск коммерческой версии **XSpider**

2004
Первый тест на проникновение

2005
Первый анализ исходного кода

2008
Выпуск нового продукта **MaxPatrol 8**

2011
Первый международный форум **Positive Hack Days**

2013
Мировой лидер по темпам роста (по версии IDC)

2014
Старт продаж линейки **Application Security (PT Application Firewall, PT Application Inspector)**

2015
Выход системы **MaxPatrol SIEM.** Первое попадание в визионеры рейтинга **Gartner Magic Quadrant (WAF)**

2016
Единственный визионер в рейтинге **Gartner Magic Quadrant (WAF).** Выход **PT ISIM** и **PT MultiScanner**

2017
Выход **PT BlackBox Scanner** и **PT Telecom Attack Discovery.** Третий год подряд визионер рейтинга **Gartner Magic Quadrant (WAF)**

Наши клиенты

POSITIVE TECHNOLOGIES

Развитие атак

и сложности индустрии SIEM

Растет разрыв между моментом компрометации и обнаружением

POSITIVE TECHNOLOGIES

62% результативных атак являются целевыми

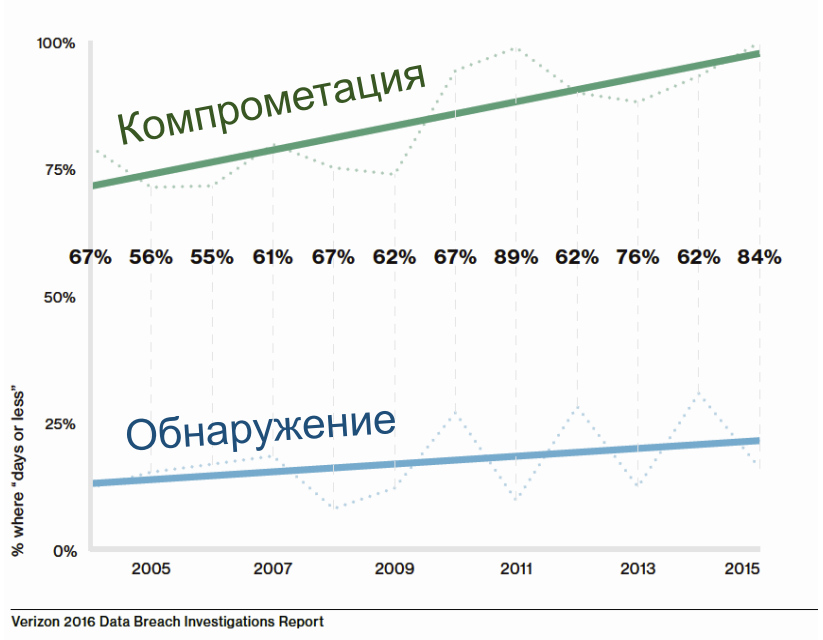
3 года в среднем злоумышленник присутствует в системе

10% атак выявляются самими жертвами

Источник: Кибербезопасность 2016–2017: от итогов к прогнозам (Positive Technologies)

Дни, часы, минуты
занимает компрометация

Недели, месяцы
проходят до обнаружения



Почему выявлять атаки становится все сложнее

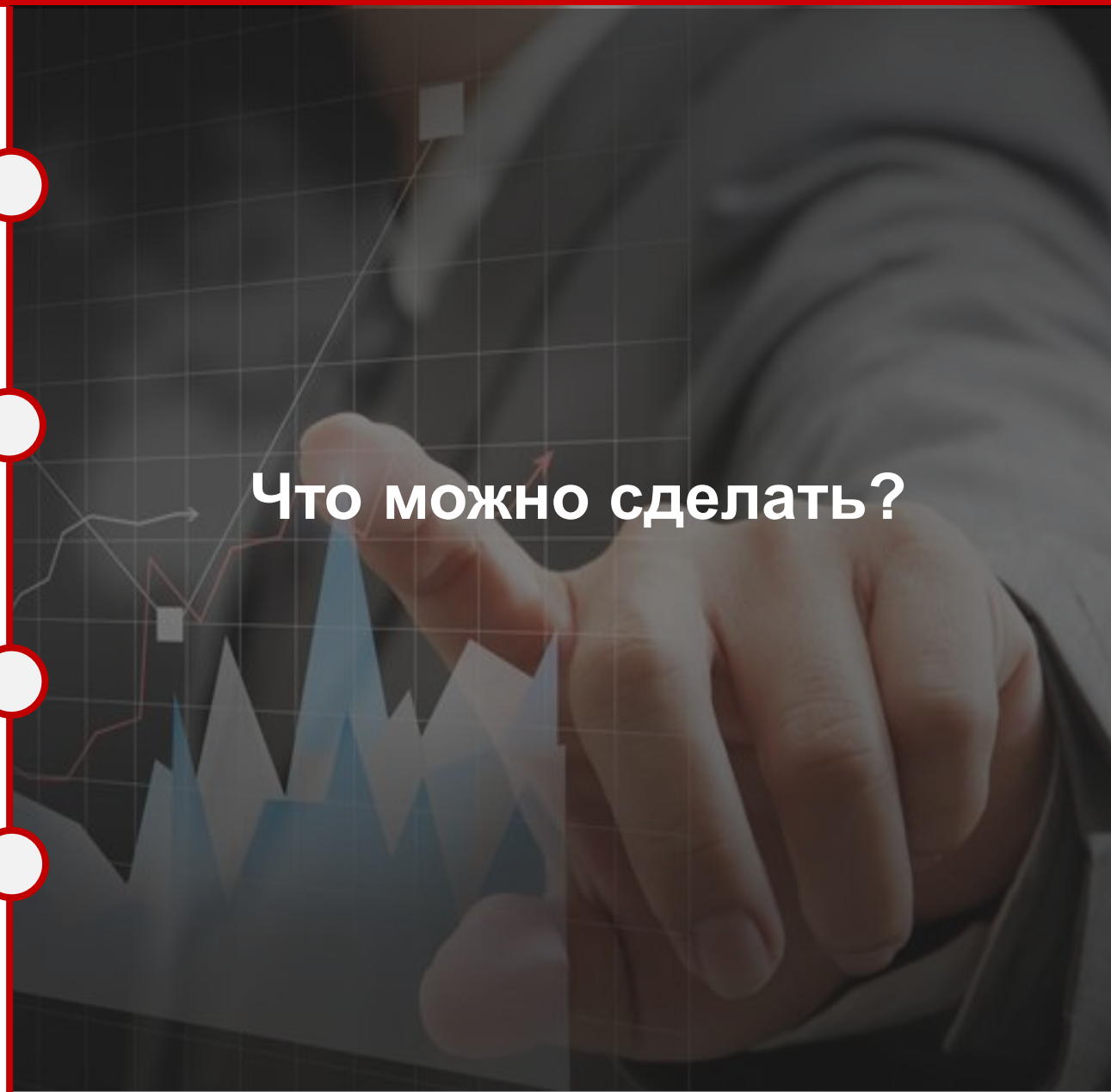
POSITIVE TECHNOLOGIES

Средства защиты, конечные и сетевые устройства создают миллионы событий, терабайты логов

Реагировать на все инциденты ИБ неэффективно: 50–95% из них составляют ложные срабатывания на СЗИ

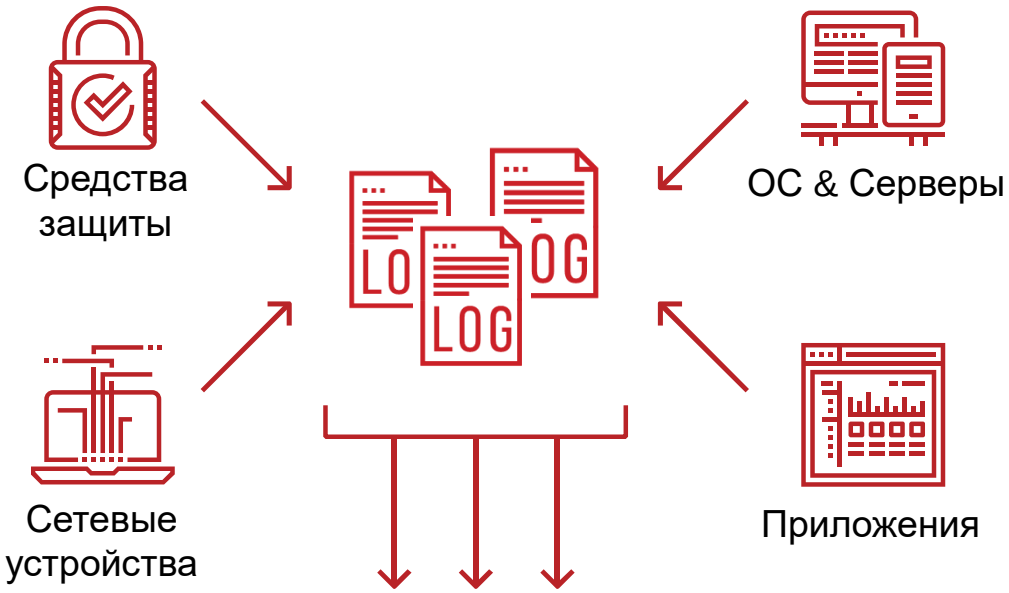
Данные с одного средства защиты не выявляют сложные и целенаправленные атаки

Инциденты разбросаны по разным системам и десяткам отчетов



Как начать выявлять инциденты

POSITIVE TECHNOLOGIES



SIEM
(security information and event management)

- Сбор событий
- Создание правил корреляции
- Выявление инцидентов

- Выбрать ключевые источники, собирать и хранить их логи
- Приоритизировать типы инцидентов с разных источников
- Настроить правила выявления атак по цепочке событий из одного или нескольких источников
- Настроить единую панель мониторинга безопасности и систему отчетности

Существующие SIEM не эффективны

POSITIVE TECHNOLOGIES

52%

организаций считают SIEM неэффективными*

68%

нанимают дополнительный персонал для анализа и реагирования на инциденты*

25%

бюджета ИБ уходит на сопровождение SIEM*

69%

ищут возможность сократить стоимость SIEM**

** Challenges to Achieving SIEM Optimization (Ponemon Institute LLC, March 2017)*
*** SIEM Efficiency Survey (Netwrix, 2016)*

Проблема на стороне SIEM, а не заказчика

POSITIVE TECHNOLOGIES

В чем проблема SIEM	Что нужно заказчику
Строит корреляции на основе ограниченных данных из логов	Видеть IT-инфраструктуру целиком и применять эффективные правила корреляции
Чувствителен к инфраструктуре	Снизить затраты на сопровождение SIEM за счет автоматической адаптации к изменениям IT-ландшафта
Эффективность SIEM напрямую зависит от экспертизы заказчика	Снизить требования к экспертизе и автоматически выявлять неизвестные угрозы

MaxPatrol SIEM:

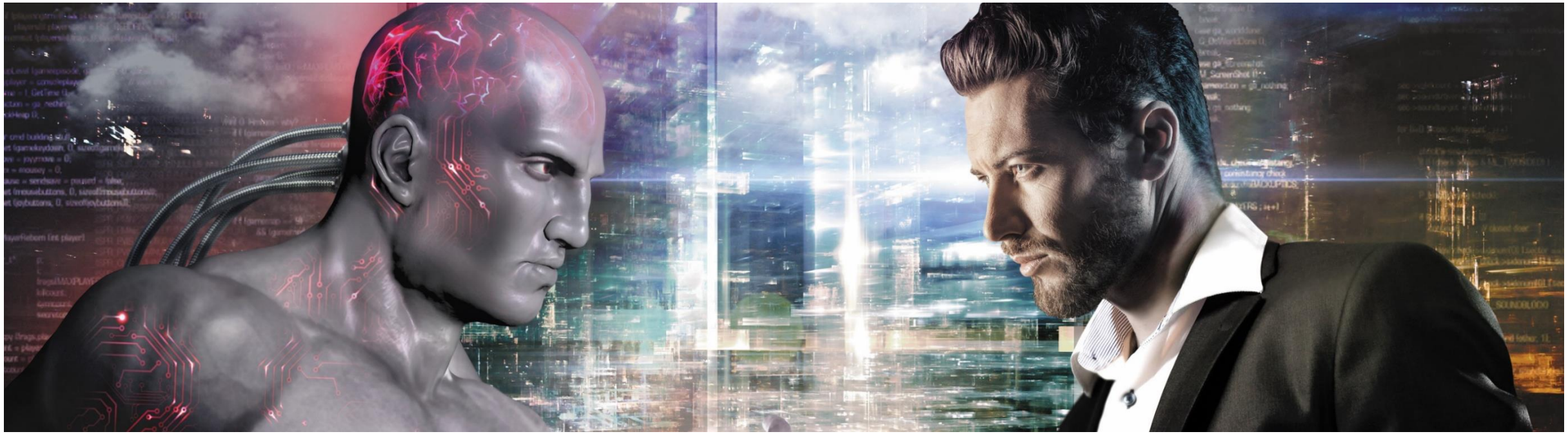
новый подход к выявлению инцидентов ИБ

MaxPatrol SIEM отвечает на современные вызовы

POSITIVE TECHNOLOGIES

MaxPatrol SIEM

- Контролирует состояние IT-инфраструктуры в любой момент времени.
- Выявляет инциденты даже после изменений IT-ландшафта.
- Автоматически поставляет ИБ-экспертизу в продукт, выявляет новые угрозы и помогает расследовать инциденты.



MaxPatrol SIEM: точная модель IT-инфраструктуры

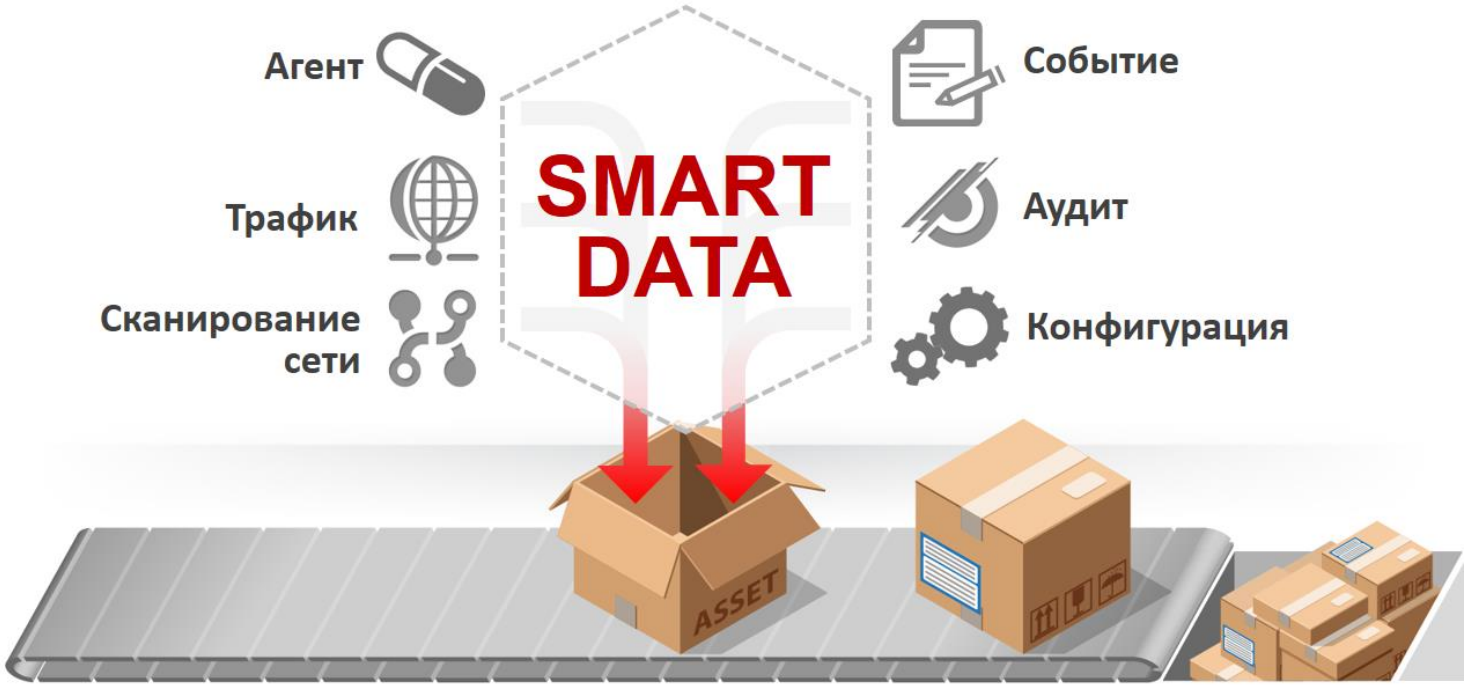
POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

- Автоматически строит полную модель IT-инфраструктуры.
- Постоянно обогащается новыми данными об IT-активах.
- Автоматически идентифицирует IT-активы даже после изменения IP- и MAC-адреса и других характеристик.

Адаптация к изменениям

Профилактика угроз



MaxPatrol SIEM: сбор данных об IT-инфраструктуре

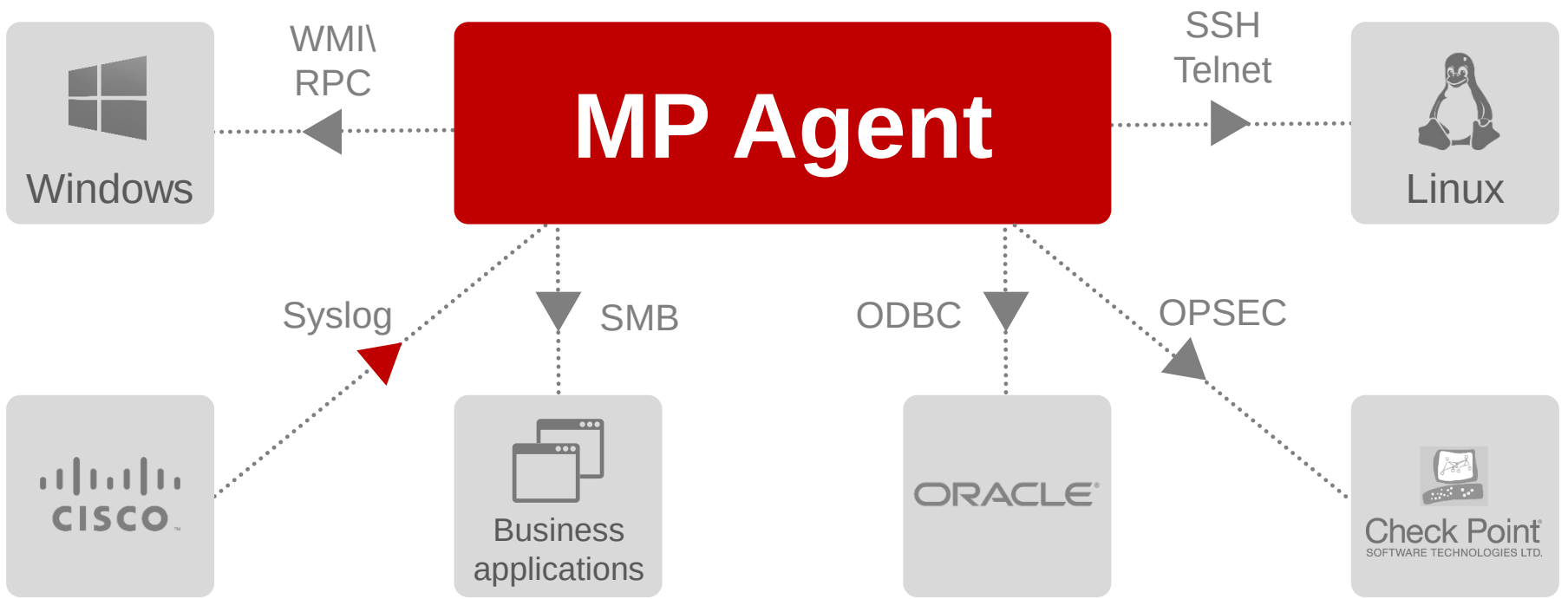
POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

- Поддержка ключевых видов транспорта.
- Собирает информацию об активах:
  - + Сканирует сеть в режимах белого и черного ящика
  - + Собирает данные из любых источников, в том числе самописных

Адаптация к изменениям

Профилактика угроз



MaxPatrol SIEM: анализ сетевого трафика

POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

Адаптация к изменениям

Профилактика угроз

Network Sensor

Анализ трафика L2-L7

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Datalink Layer
- Physical Layer

Наполняет конфигурации активов

Обнаруживает новые активы

Обогащает SIEM событиями о сетевых взаимодействиях

MaxPatrol SIEM: анализ данных с конечных устройств

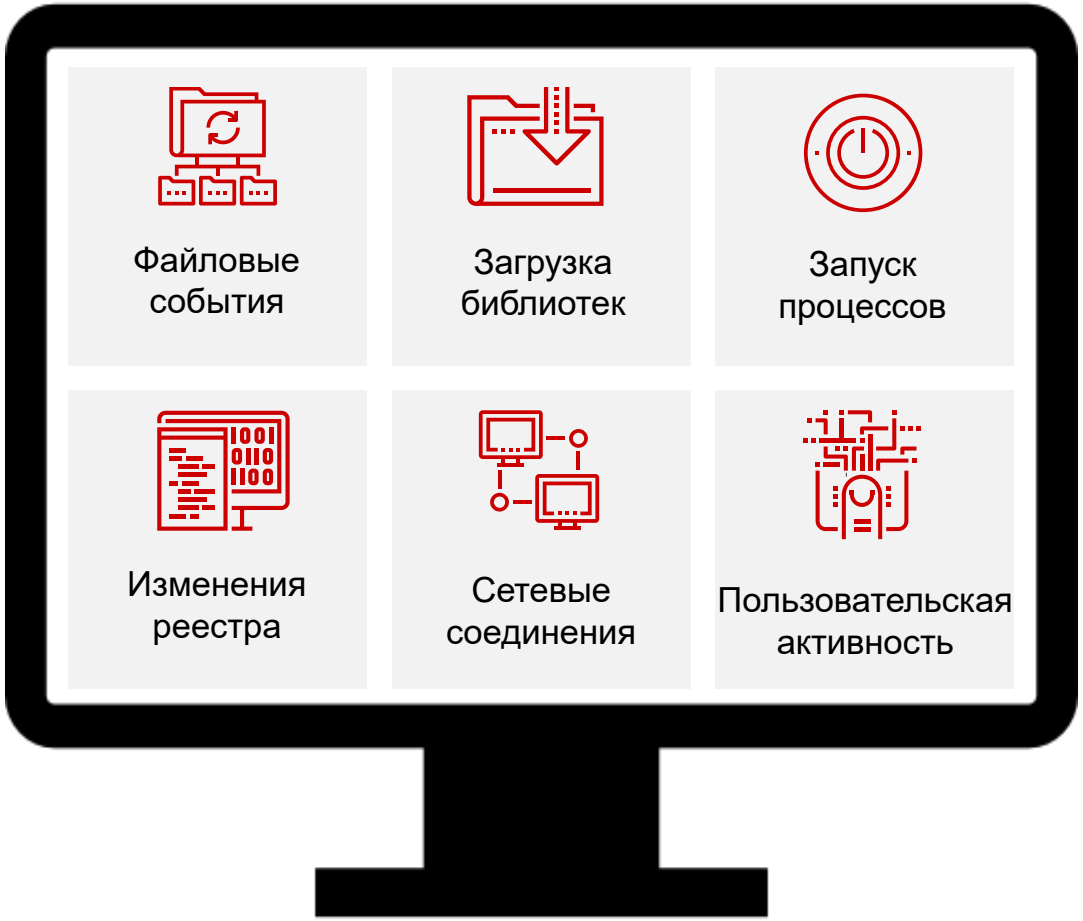
POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

Адаптация к изменениям

Профилактика угроз

Endpoint Monitor



- Выявляет потенциально опасные действия
- Обнаруживает атаки на ранних этапах
- Обнаруживает активность вредоносного ПО

MaxPatrol SIEM: полная и точная модель IT-активов

POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

Адаптация к изменениям

Профилактика угроз

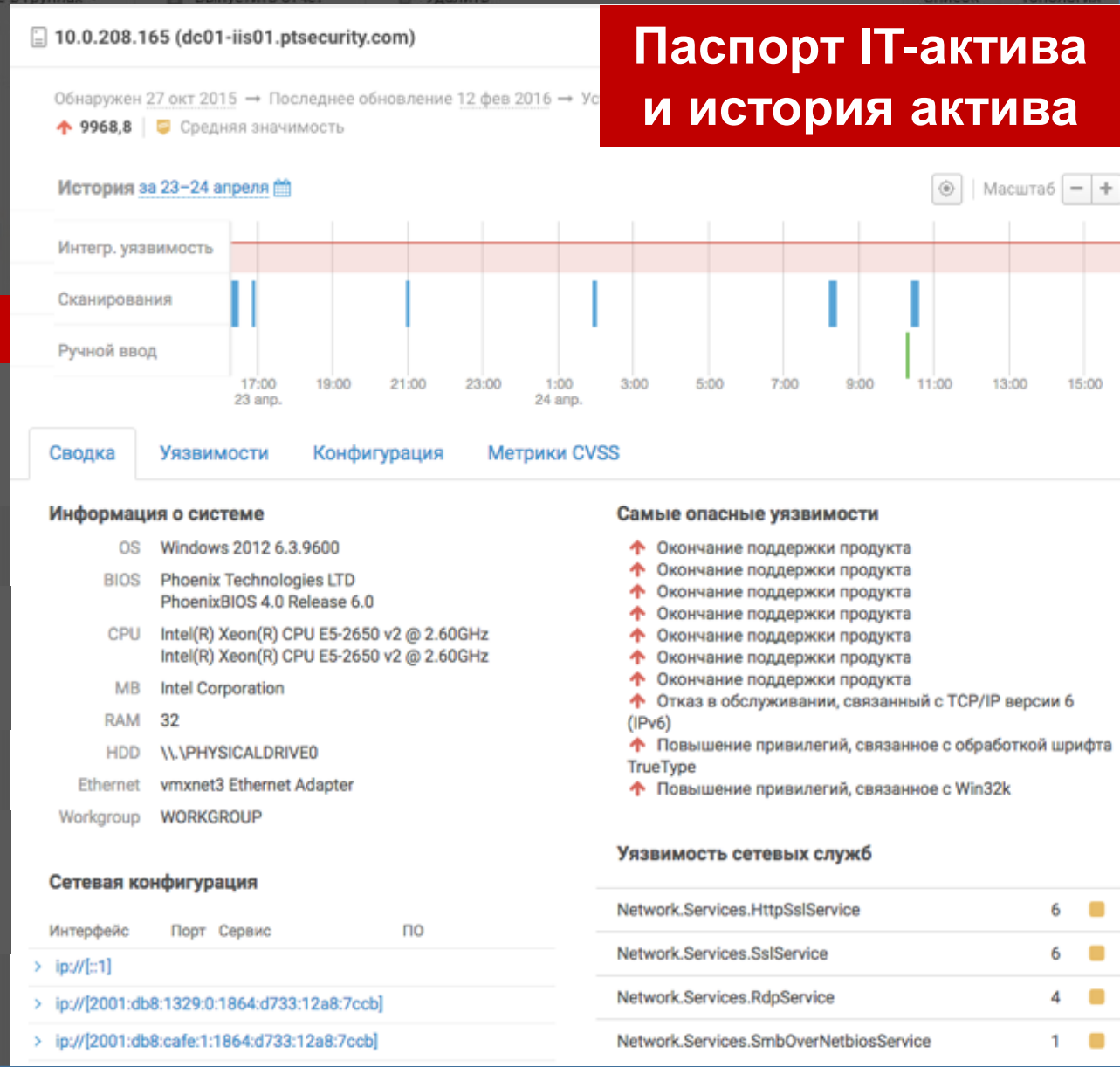
MaxPatrol SIEM:

Упорядочивает данные об инфраструктуре в IT-активы и их взаимодействия

Автоматически присваивает значимость IT-активам и приоритизирует на ее основе инциденты

Собирает и хранит не логи, а состояния каждого IT-актива во времени

Паспорт IT-актива и история актива



MaxPatrol SIEM: группировка IT-активов по любым признакам

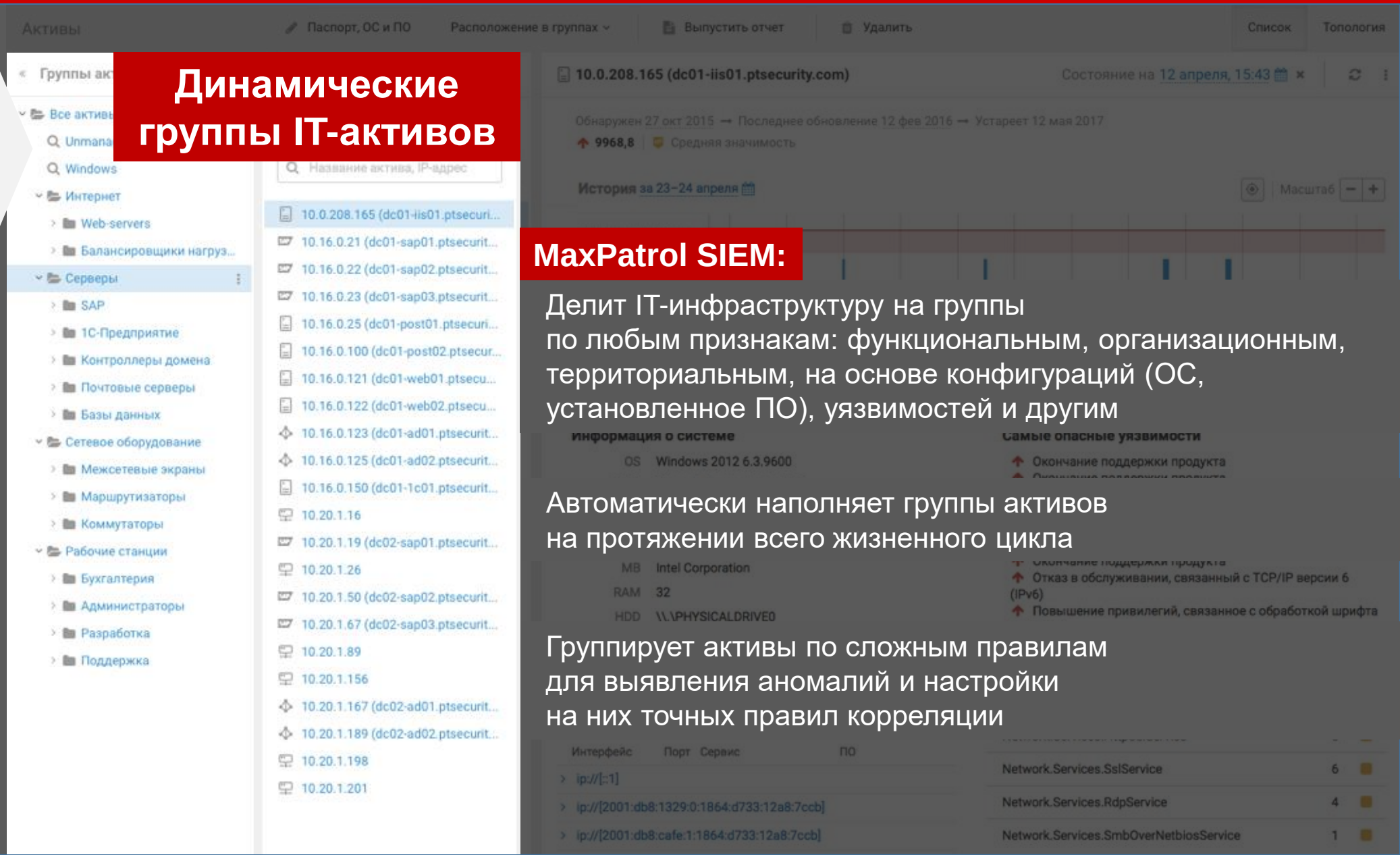
POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

Адаптация к изменениям

Профилактика угроз

Динамические группы IT-активов



MaxPatrol SIEM:

Делит IT-инфраструктуру на группы по любым признакам: функциональным, организационным, территориальным, на основе конфигураций (ОС, установленное ПО), уязвимостей и другим

Автоматически наполняет группы активов на протяжении всего жизненного цикла

Группирует активы по сложным правилам для выявления аномалий и настройки на них точных правил корреляции

MaxPatrol SIEM: сетевая достижимость

POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

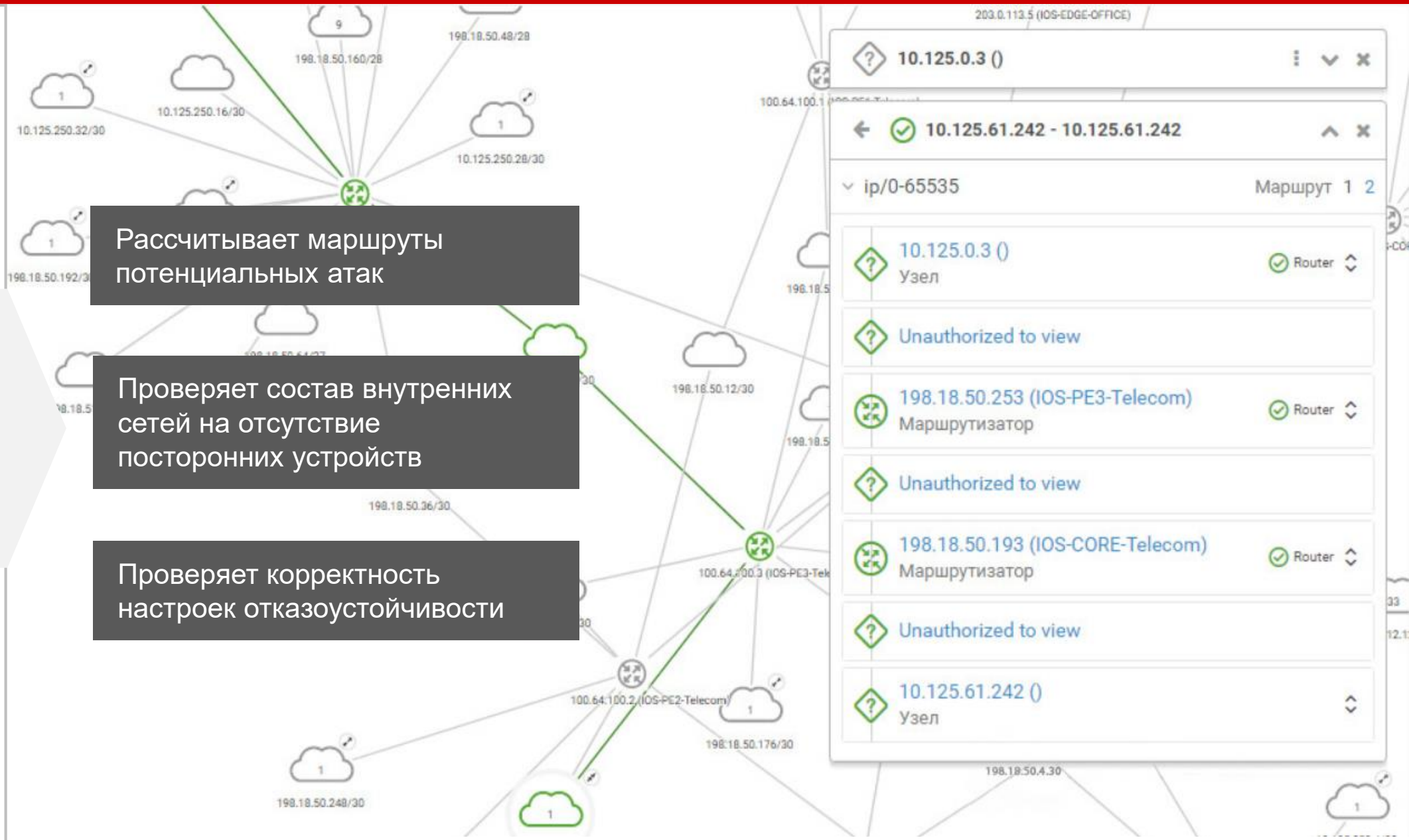
Адаптация к изменениям

Профилактика угроз

Рассчитывает маршруты потенциальных атак

Проверяет состав внутренних сетей на отсутствие посторонних устройств

Проверяет корректность настроек отказоустойчивости



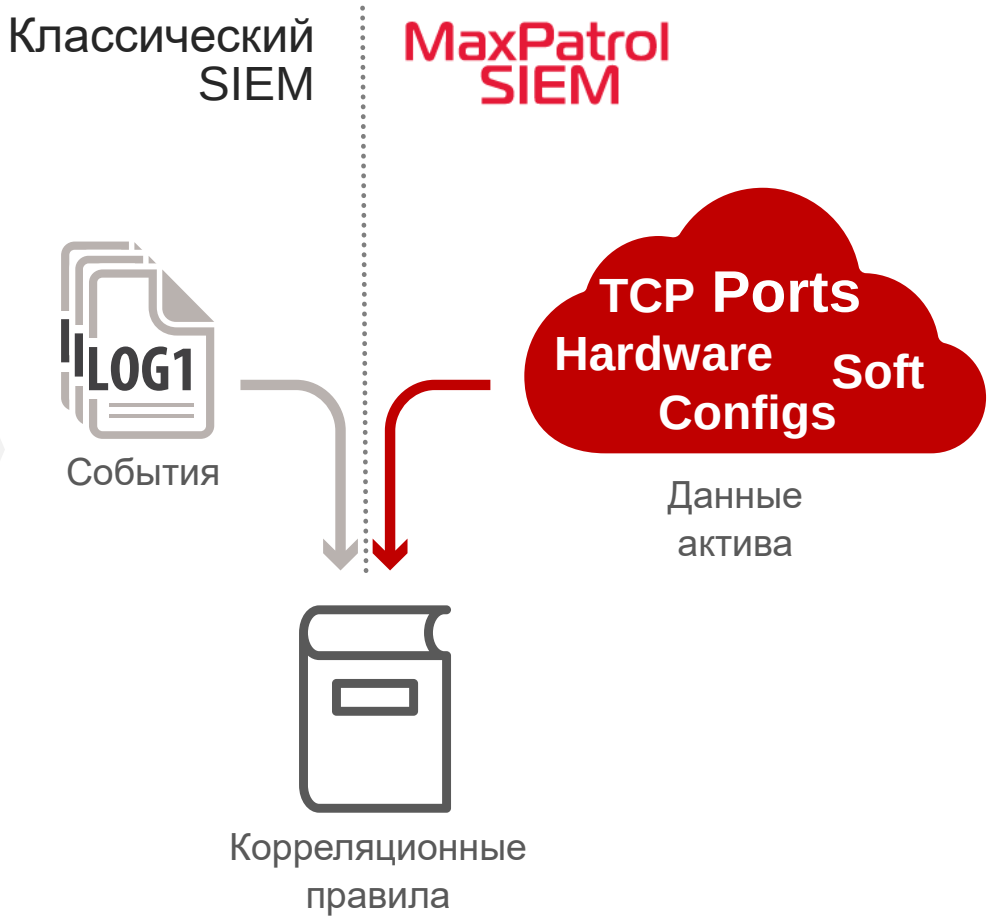
MaxPatrol SIEM: модельные корреляции

POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

Адаптация к изменениям

Профилактика угроз



MaxPatrol SIEM автоматически адаптируется к изменениям IT-ландшафта.

Создает корреляции на основе данных IT-активов и динамических групп активов, а не логов.

Правила корреляции продолжают выявлять угрозы после появления нового оборудования или изменения конфигурации сетевых узлов.

PT KB: профилактика угроз и ИБ-экспертиза в вашей SIEM

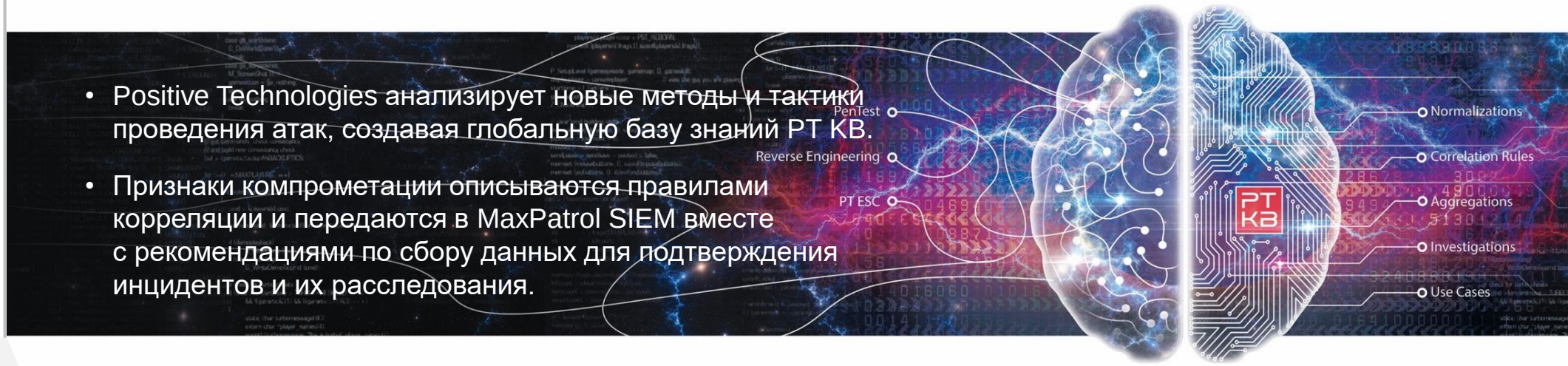
POSITIVE TECHNOLOGIES

Контроль
IT-инфраструктуры

Адаптация
к изменениям

Профилактика угроз

Positive Technologies Knowledge Base



- Positive Technologies анализирует новые методы и тактики проведения атак, создавая глобальную базу знаний PT KB.
- Признаки компрометации описываются правилами корреляции и передаются в MaxPatrol SIEM вместе с рекомендациями по сбору данных для подтверждения инцидентов и их расследования.

- 15 лет масштабных тестов на проникновение.
- 1500 найденных уязвимостей корпоративных сетей ежегодно.
- Более 200 аудитов безопасности корпоративных систем ежегодно.
- PT ESC — более 50 расследований взломов инфраструктуры ежегодно.
- Аналитика и моделирование атак.
- Прототипирование и испытание технологий.

MaxPatrol SIEM: в каждом пакете обновлений PT KB

POSITIVE TECHNOLOGIES

Контроль
IT-инфраструктуры

Адаптация
к изменениям

**Профилактика
угроз**

Новые правила
корреляции, агрегации,
нормализации

Рекомендации по сбору
информации из MP SIEM
для подтверждения инцидента
и его расследования

PT
KB

Информация о методах
и тактиках проведения атак,
индикаторы компрометации

Рекомендации по тонкой
настройке аудита на источниках
для точного выявления атак

MaxPatrol SIEM: преимущества PT KB в SIEM для бизнеса

POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

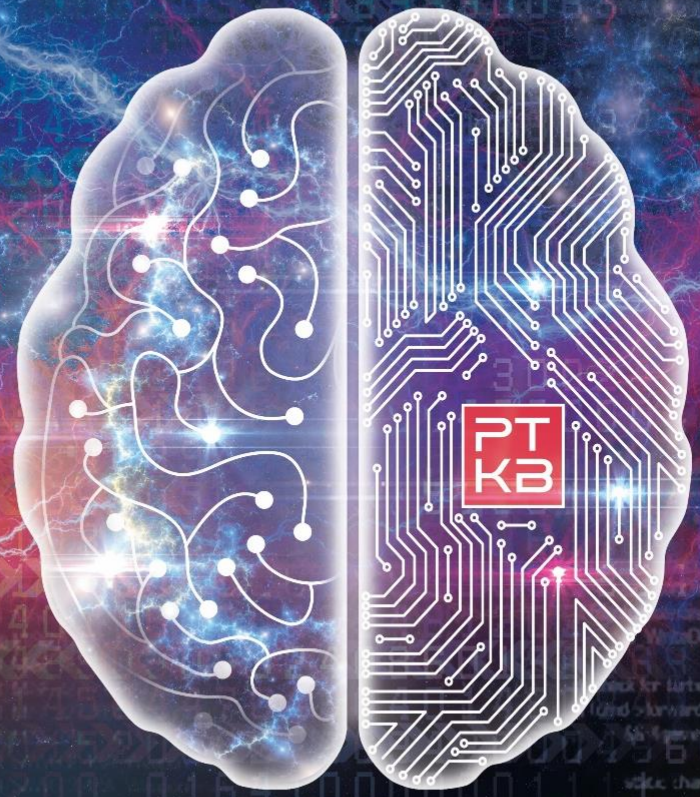
Адаптация к изменениям

Профилактика угроз

Профилактика новых угроз и массовых атак

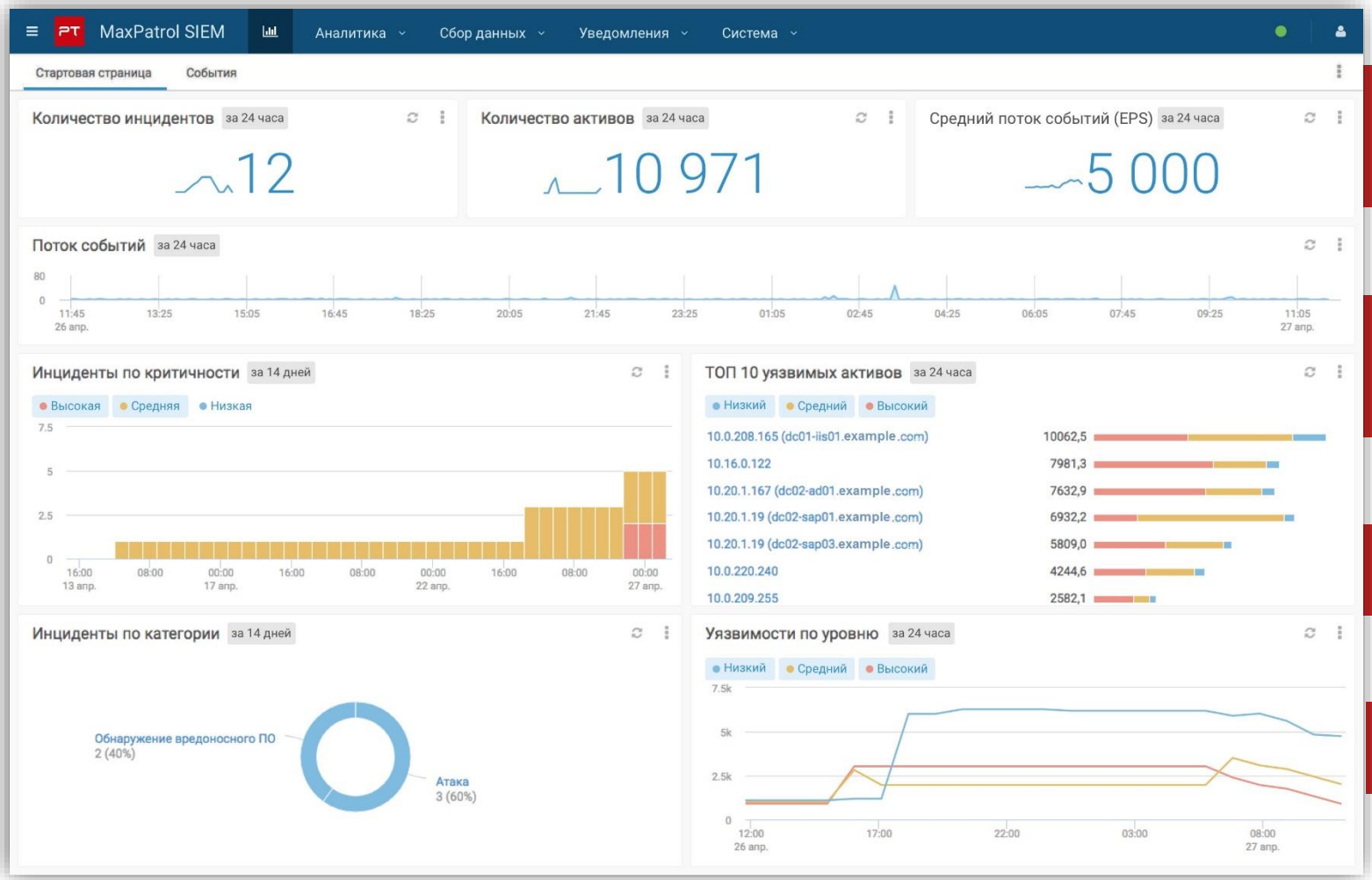
Выявление целенаправленных атак

Снижение требований к экспертизе команды эксплуатации SIEM



MaxPatrol SIEM: визуализация и отчетность

POSITIVE TECHNOLOGIES



Настраиваемые дашборды
и пользовательские виджеты

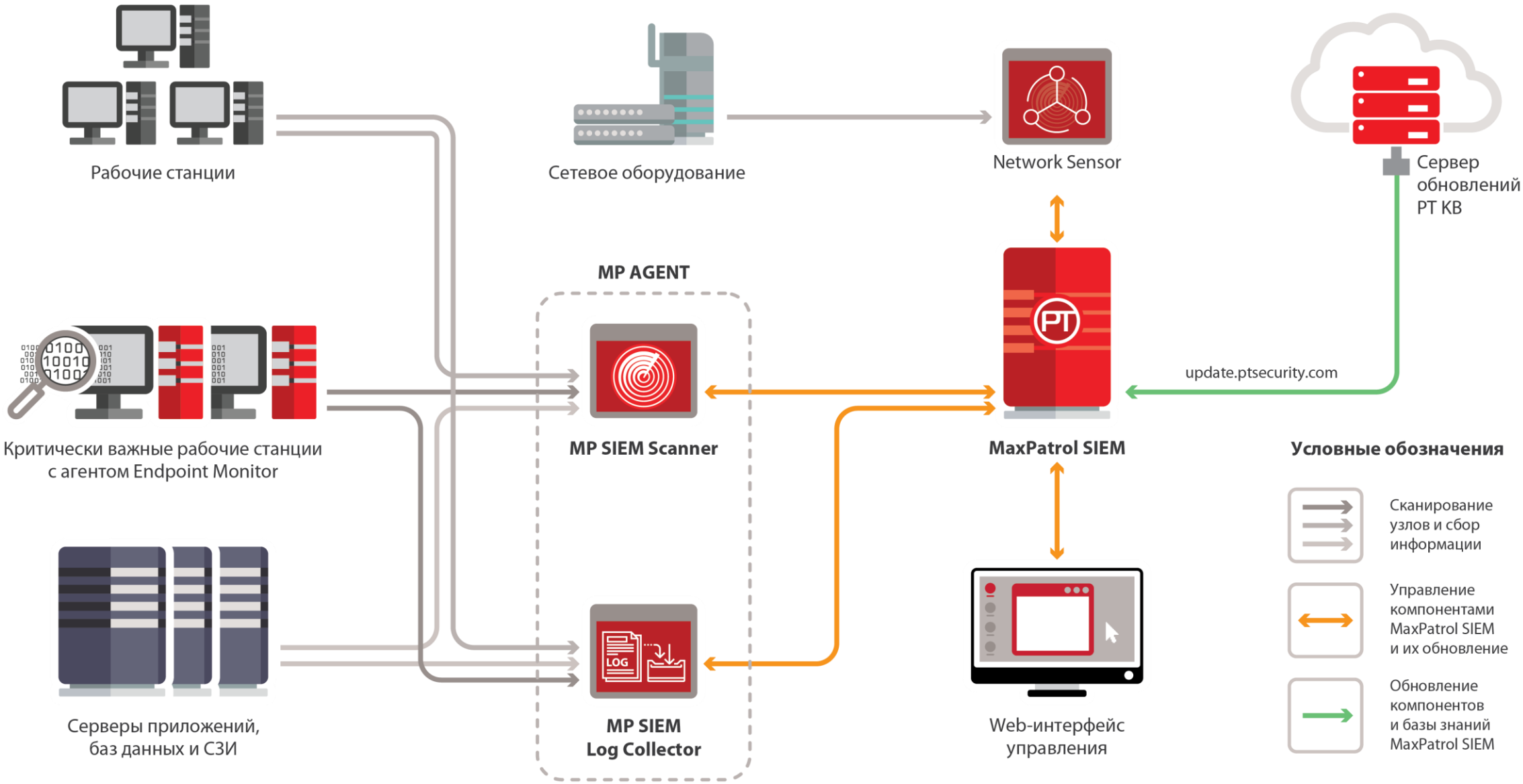
Детализация информации
с дашбордов в один клик

Автоматическое создание отчетов

Отправка отчетов по расписанию

MaxPatrol SIEM: архитектура системы

POSITIVE TECHNOLOGIES



Почему MaxPatrol SIEM

Преимущества MaxPatrol SIEM

POSITIVE TECHNOLOGIES

Характеристика	MaxPatrol SIEM	Другие SIEM
Сбор и управление данными		
Безагентный сбор логов	+	+
Агент для сбора низкоуровневой информации с конечных точек	+	+/– (сторонние решения, $)
Сбор и анализ сетевой активности	+	+/– (сторонние решения, $)
Автоматическое обнаружение IT-активов и управление активами	+	+/– (сторонние решения, $)
Автоматическое построение топологии сети и ее актуализация в режиме реального времени	+	–
Выявление инцидентов		
Корреляция событий безопасности	+	+
Автоматическая адаптация к изменениям, модельные корреляции	+	–
Выявление инцидентов на основе сетевой достижимости	+	–
Обнаружение новых угроз за счет автоматической передачи ИБ-экспертизы в продукт	+	–
Другое		
Визуализация и отчеты по событиям и инцидентам	+	+
Открытый стандартизированный API-интерфейс для интеграции с другими решениями	+	+/– (частично, $)
Бесплатное покрытие актуальных источников логов	+	+/–
Состоит в реестре российского ПО, сертифицирован ФСТЭК и Минобороны РФ	+	+/–

Заказчики MaxPatrol SIEM

POSITIVE TECHNOLOGIES

Более 50 проектов с 2015 года

- Министерство транспорта
- ФТС России
- Министерство энергетики
- Росатом
- Роснефть
- Росэнергоатом
- ДИТ Москвы
- ФНС
- ГТЛК

MaxPatrol SIEM: отзывы

POSITIVE TECHNOLOGIES

Больше 1000
площадок информатизации

Больше 150 000 узлов сети

«С MaxPatrol SIEM мы получили возможность автоматизировать работу с большими данными антивирусной системы в ФНС России и в результате сократили время на эскалацию инцидентов и реагирование на них».

Юшков Дмитрий Юрьевич,
Заместитель начальника Межрегиональной инспекции Федеральной налоговой службы по централизованной обработке данных

Меньше 6 месяцев
длилось внедрение

«Успешное внедрение системы MaxPatrol SIEM создало дополнительный механизм для эффективного управления процессом обеспечения информационной безопасности».

Алексей Щербаков,
Заместитель генерального директора ПАО «Государственная транспортная лизинговая компания»

Выполнение требований регуляторов

POSITIVE TECHNOLOGIES

- Защита персональных данных (ФЗ-152, Приказ ФСТЭК №21)
- Защита государственных информационных систем (Приказ ФСТЭК №17)
- Защита АСУ ТП (Приказ ФСТЭК №31)

Сертификат ФСТЭК России № 3734 от 12 апреля 2017 г. позволяет применять MaxPatrol SIEM для защиты АС до 1Г, ИСПДн, ГИС и АСУ ТП.

- Требования СТО БР ИББС и рекомендации РС БР ИББС-2.5-2014
- Федеральный закон «О национальной платежной системе» 161-ФЗ (Положение № 382-П)
- Требования PCI DSS

MaxPatrol SIEM входит в реестр Российского ПО, № 1143 от 14 июня 2016 г. (https://reestr.minsvyaz.ru/reestr/79129/)

Сертификат МО № 3044 от 14 января 2016 г. позволяет применять MaxPatrol SIEM для защиты сетей Министерства обороны РФ.

MaxPatrol SIEM LE

POSITIVE TECHNOLOGIES

Программно-аппаратный комплекс с единой техподдержкой

- **Самый быстрый и доступный** способ для малых и средних организаций получить полноценную систему выявления инцидентов ИБ.
- Включает все необходимое для сбора и анализа данных **в небольших инфраструктурах** в 250, 500 или 1000 сетевых узлов.

Сравнение MaxPatrol SIEM LE и MaxPatrol SIEM

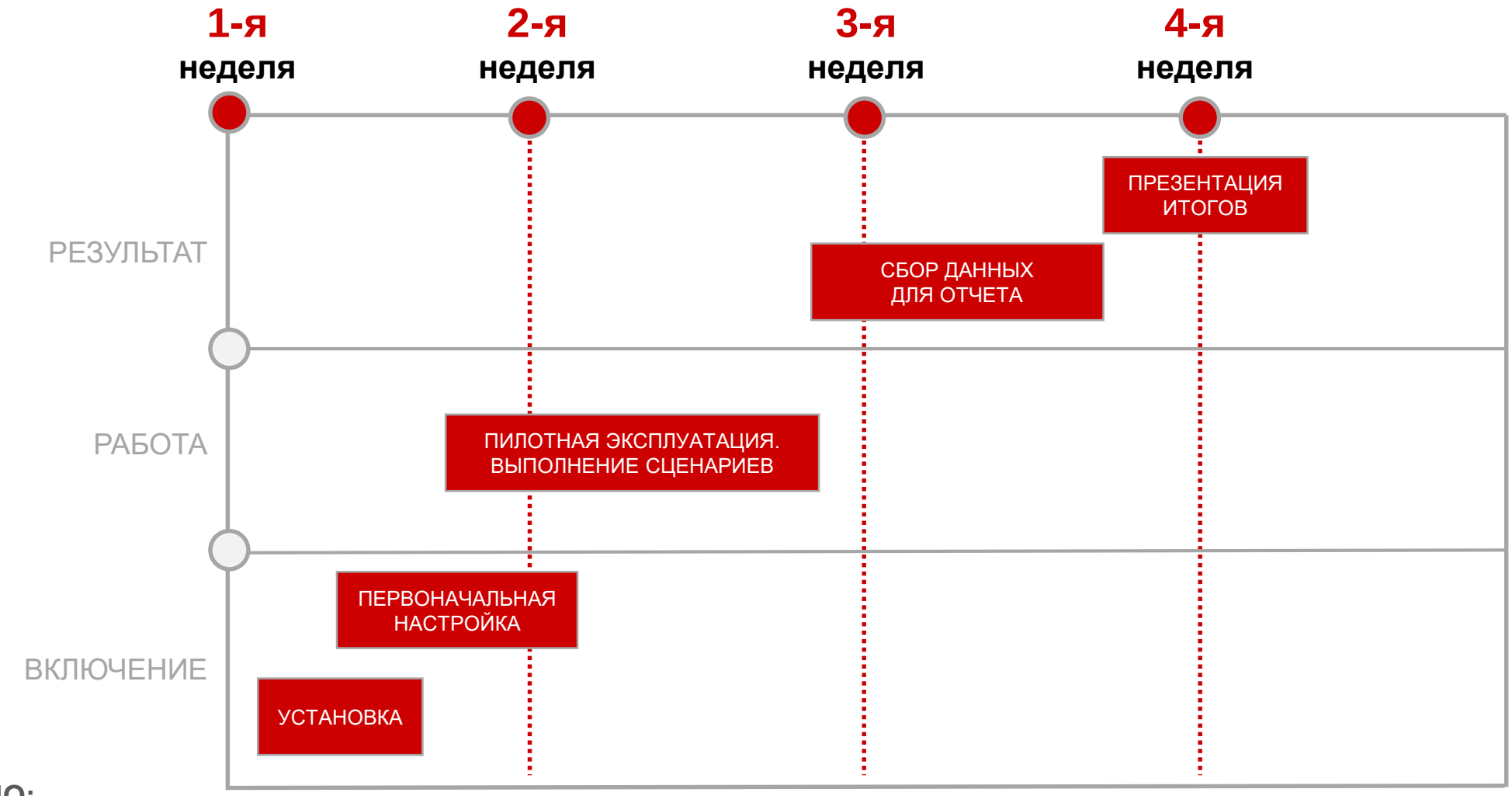
POSITIVE TECHNOLOGIES

Характеристика	MaxPatrol SIEM LE	MaxPatrol SIEM
Аппаратная платформа включена в состав продукта	+	–
Конфигурация для организаций с небольшим количеством сетевых узлов (250 или 500)	+	–
Подключение актуальных источников силами Positive Technologies	+	+
Не содержит ограничений по производительности (EPS)	+	+
Масштабируемость, распределенная конфигурация	–	+
Конфигурация для организаций с общим количеством сетевых узлов больше чем 1000	–	+
Увеличение хранилища для больших объемов данных и длительного хранения (ограниченно доступно в виде опции архивного хранения для MaxPatrol SIEM LE)	+	+

Пилотный проект

Примерный план пилотного проекта

POSITIVE TECHNOLOGIES



ВАЖНО:

- До начала работ получить список сценариев использования, которые заказчик хочет проверить.
- При необходимости подключить нестандартные источники, сроки настройки и выполнения сценариев увеличатся.

MaxPatrol SIEM: принципы лицензирования

POSITIVE TECHNOLOGIES

Основная лицензия	Основная лицензия на общее количество сетевых узлов* организации (на 1, 2, 5, 10, 20, 50 или 100 тысяч)	
+		
Инфраструктурные лицензии	MP SIEM Server	Управляющий сервер
	MP SIEM Scanner	Модуль сканирования активов
	MP SIEM Log Collector	Модуль сбора событий
	MP SIEM Network Sensor	Модуль сбора и анализа сетевого трафика
	MP SIEM Endpoint Monitor	Модуль сбора системных событий ОС Windows и мониторинга сетевых служб

ЧЕСТНОЕ ЛИЦЕНЗИРОВАНИЕ:

- Без привязки к производительности (EPS)
- Без ограничения количества источников событий на одном сетевом узле

MaxPatrol SIEM LE
Лицензии на 250, 500 или 1000 узлов

** Под сетевым узлом подразумевается любой элемент IT-инфраструктуры, подключенный к сети: серверы, компьютеры, принтеры, IP-телефония и пр.*


Спасибо!
POSITIVE TECHNOLOGIES
ptsecurity.com