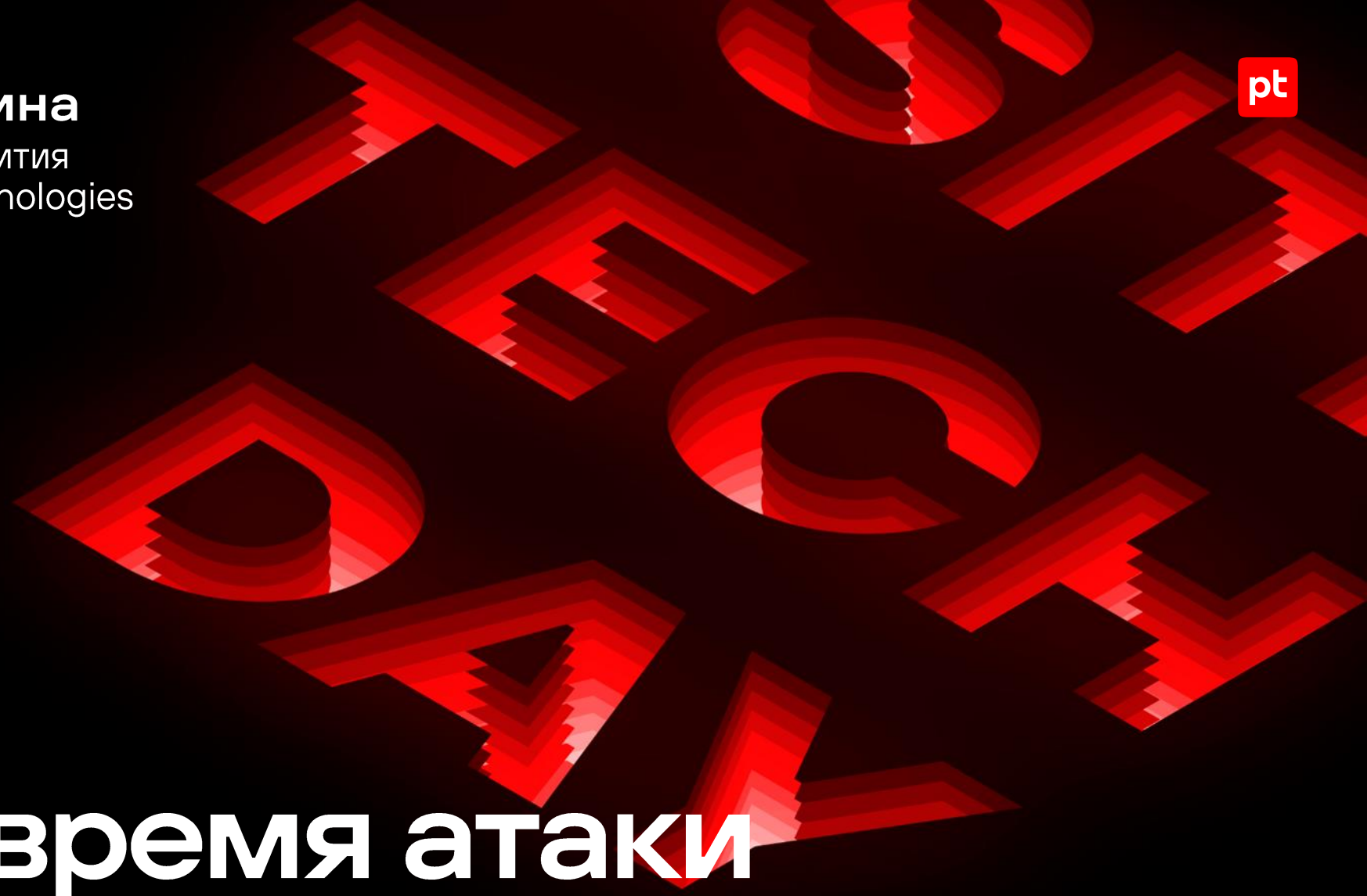
Анастасия Важенина
Руководитель практики развития
метапродуктов Positive Technologies



До и во время атаки

Как метапродукты помогают департаментам
ИТ и ИБ противостоять хакерам

Анастасия Важенина

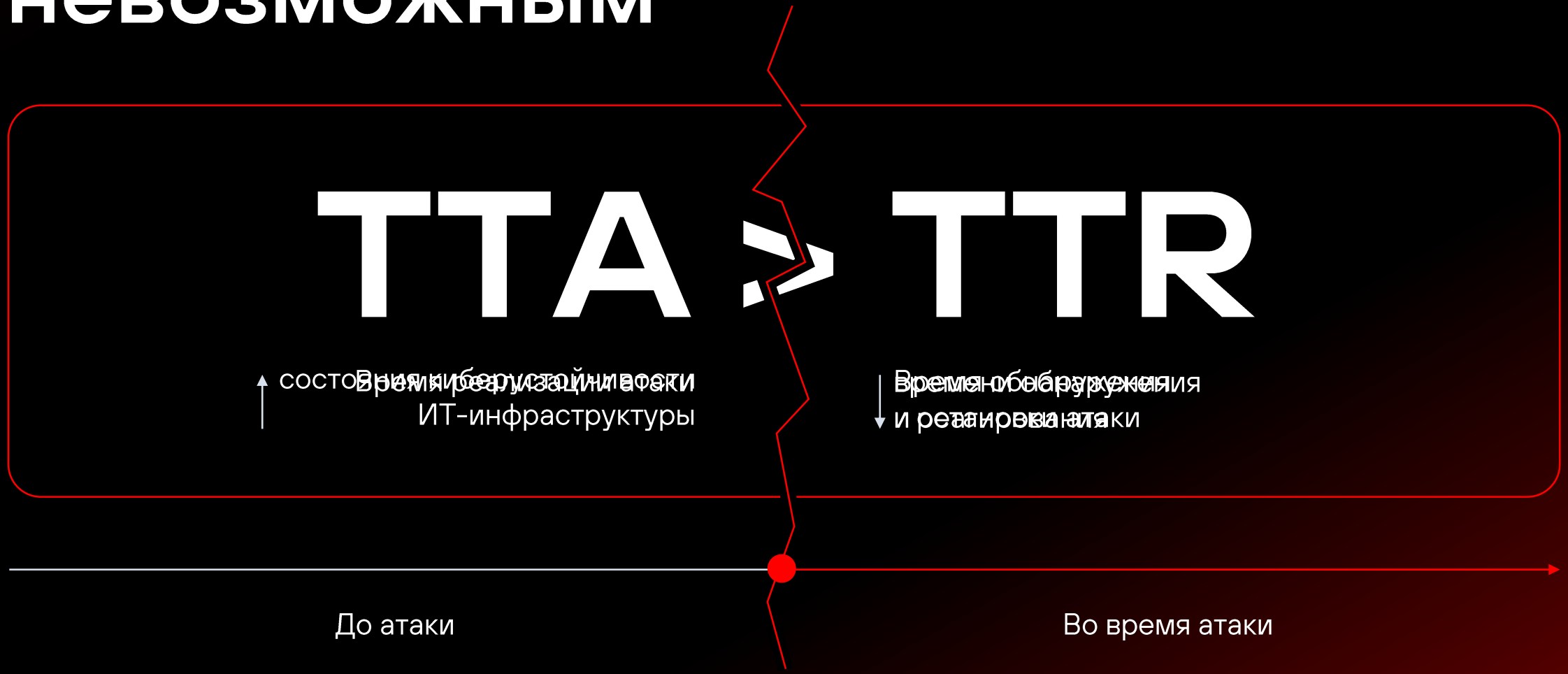
Руководитель практики развития
метапродуктов Positive Technologies

15+ лет — в сфере ИБ

11+ лет — в разработке

3+ года
- автоматизация ИБ
- реагирование на инциденты
- оркестрация средств защиты

Цель кибербезопасности — сделать недопустимое невозможным



До атаки

> Цель:

максимизировать время атаки (TTA)↑

> Задачи:

- Понять, что у нас есть
- Определить, какие есть проблемы
- Исправить ситуацию

Что у нас есть

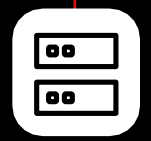
ИТ-инфраструктура

Что у нас есть

Asset management

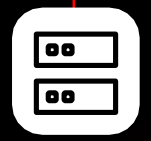
- Активы
- Сетевые доступы
- Программное обеспечение
- Пользователи

ИТ-инфраструктура



Серверное оборудование

Рабочие станции



Сетевое оборудование

Системное ПО

Прикладное ПО

Какие есть проблемы

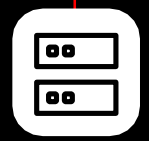
Слабости

- Misконфигурации ПО
- Избыточные сетевые доступы
- Уязвимости
- Избыточные привилегии пользователей

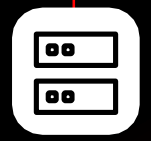
Asset management

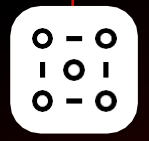
- Активы
- Сетевые доступы
- Программное обеспечение
- Пользователи

ИТ-инфраструктура


Серверное оборудование

Рабочие станции


Сетевое оборудование


Системное ПО

Прикладное ПО

Исправить ситуацию

Список рекомендаций для всей ИТ-инфраструктуры

Обновление и переконфигурация ПО	Изменение параметров сети	Патчинг уязвимостей	Ограничение прав пользователей

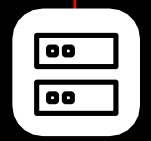
Слабости

Misконфигурации ПО	Избыточные сетевые доступы	Уязвимости	Избыточные привилегии пользователей

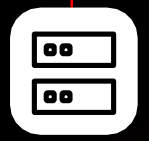
Asset management

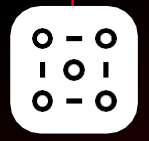
Активы	Сетевые доступы	Программное обеспечение	Пользователи

ИТ-инфраструктура


Серверное оборудование

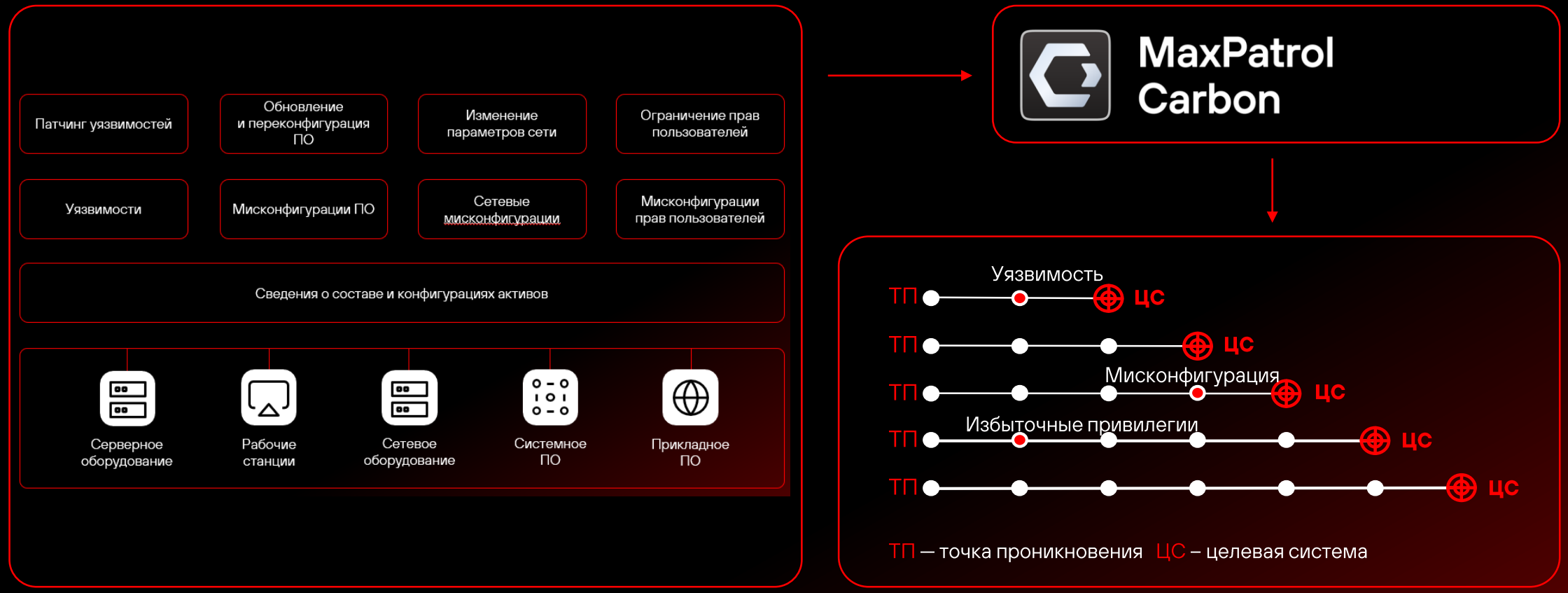
Рабочие станции


Сетевое оборудование


Системное ПО

Прикладное ПО

От отдельных слабостей к маршрутам атак

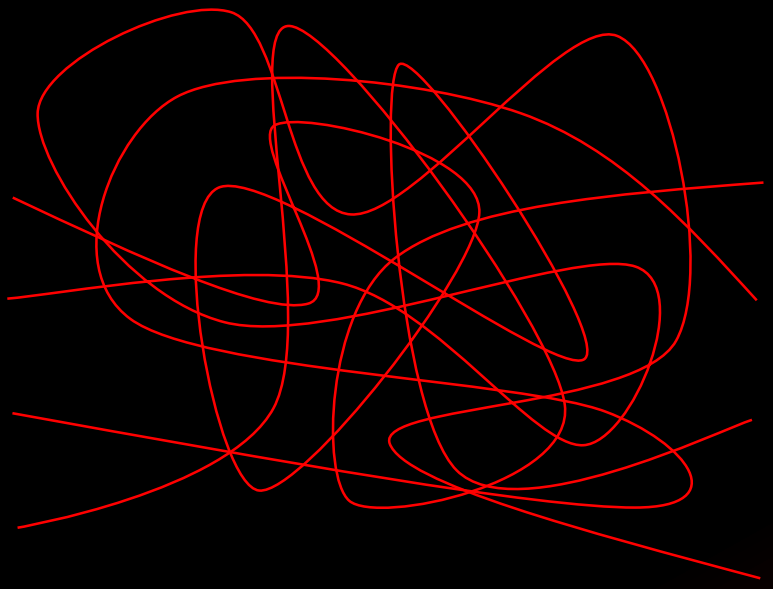


Бизнес-ориентированный подход

Подход к обеспечению киберустойчивости ИТ-инфраструктуры с фокусом на неприемлемые риски

Точка проникновения в инфраструктуру:

- Веб-приложения
- Wi-fi сети
- Компьютеры сотрудников
- VPN-подключение

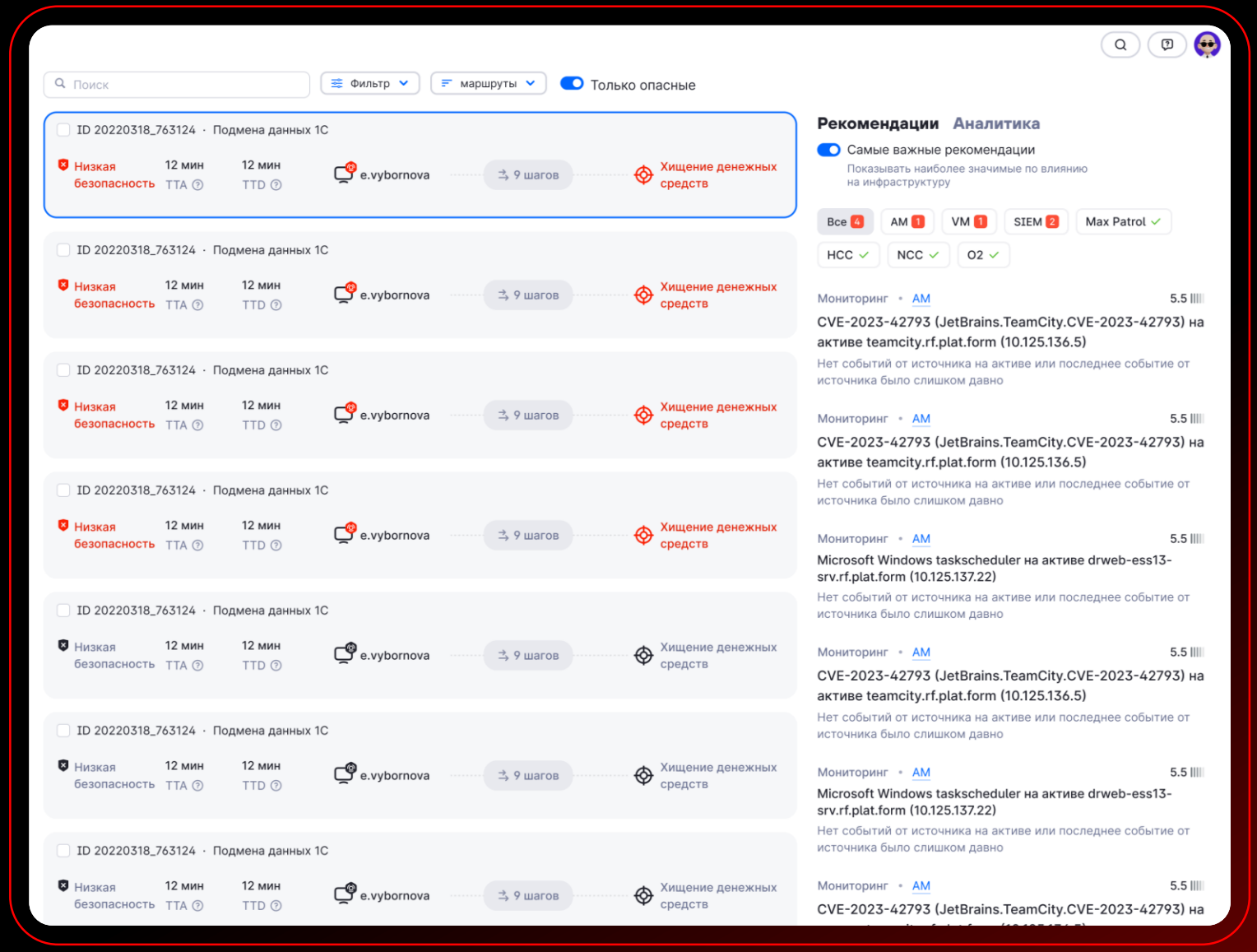


Неприемлемые риски:

- Кража коммерческой тайны
- Кража денежных средств
- Нарушение производственных процессов
- Компрометация данных

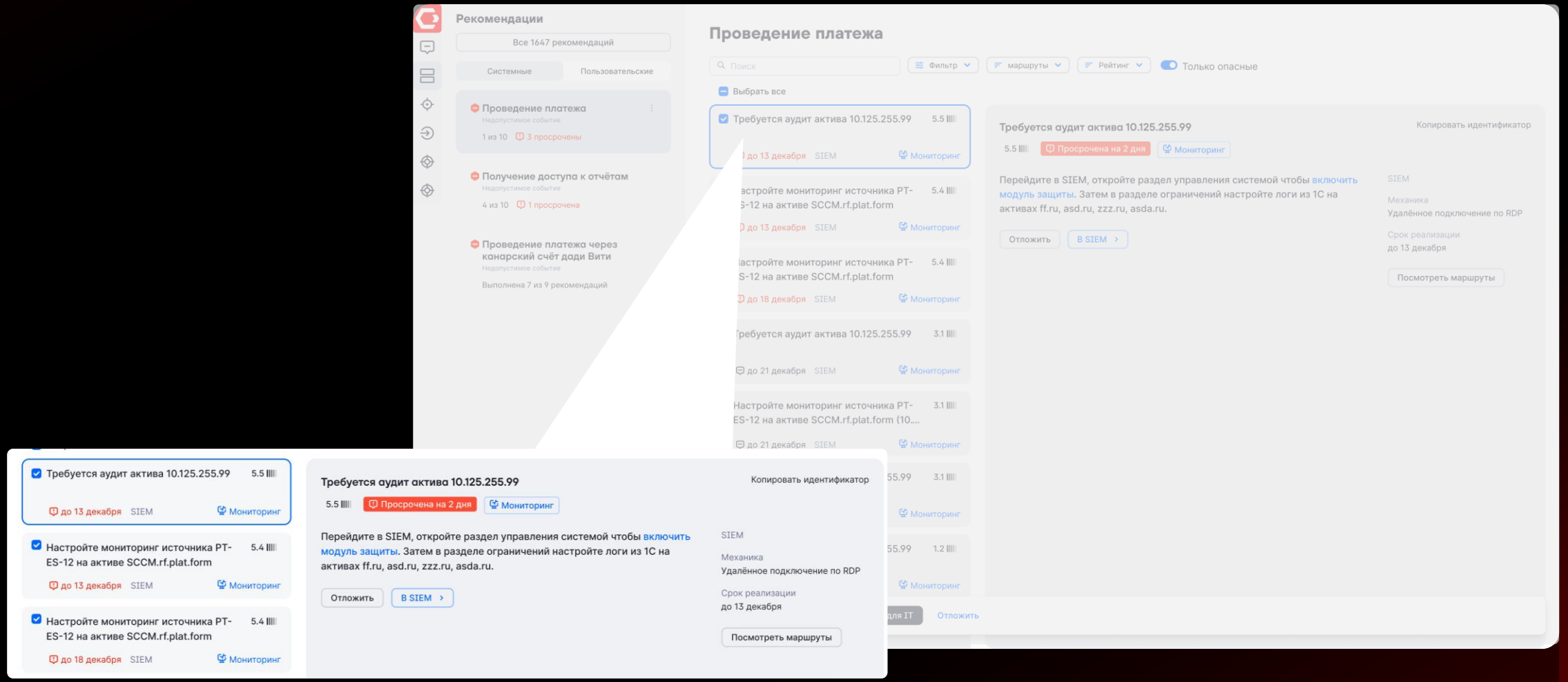
MaxPatrol Carbon

Маршруты атак



План действий готов

Приоритетный список задач



Результаты MaxPatrol Carbon

> Задача

Анализ инфраструктуры со 100+ активами и 150+ учетными записями и моделирование возможных действий злоумышленников

Результат

>200 000
маршрутов атак

от 1 до 27 шагов
в маршруте

11 минут
самый быстрый маршрут

4 приоритетных рекомендации
для устранения всех одношаговых маршрутов до реализации недопустимых событий

MaxPatrol Carbon

- Выявление в режиме реального времени потенциально возможных марштуров атак на ключевые ИТ-активы компании
- Приоритизация задач с учетом рисков для бизнеса
- Формирование четких рекомендаций, что необходимо сделать для повышения уровня защищенности ИТ-инфраструктуры
- Обоснование для ИТ-департамента необходимости выполнять определенные работы

Во время атаки

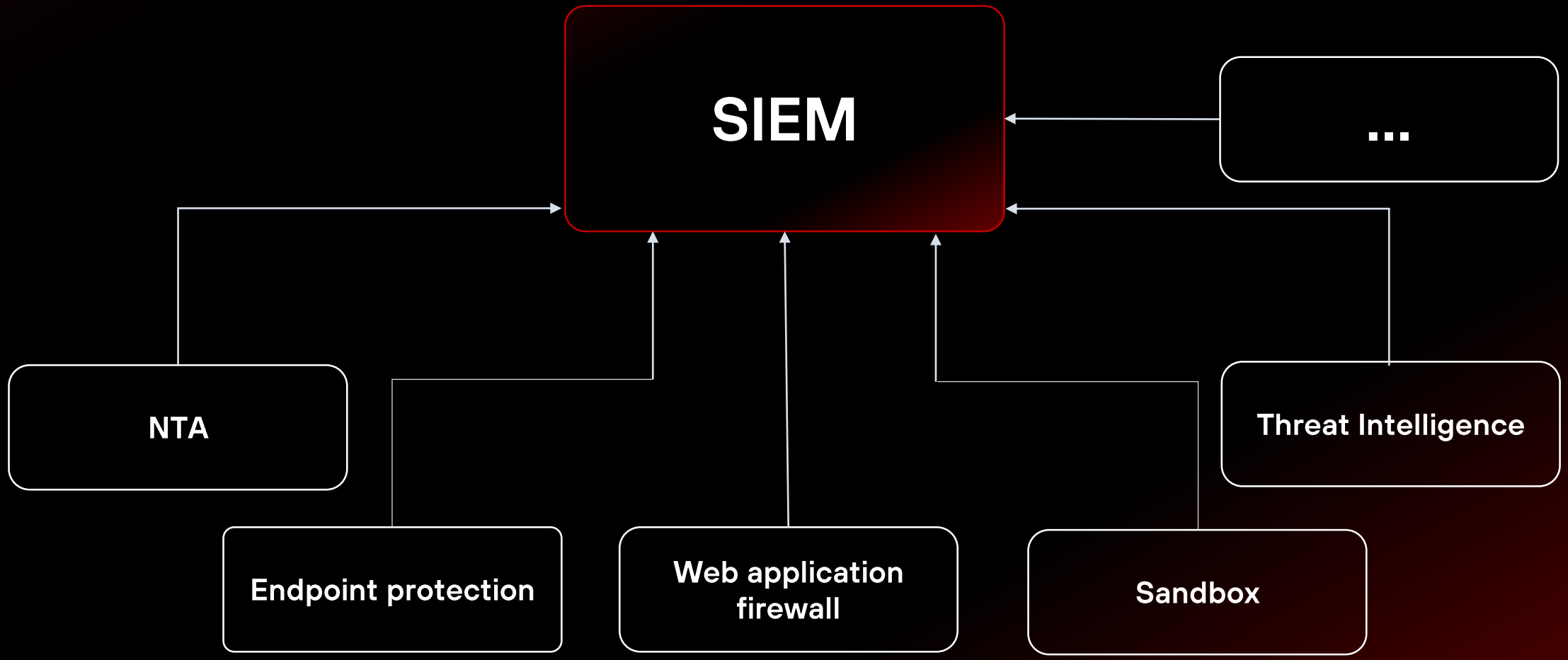
> Цель:

минимизировать время обнаружения и реагирования на атаку (TTR)↓

> Задачи:

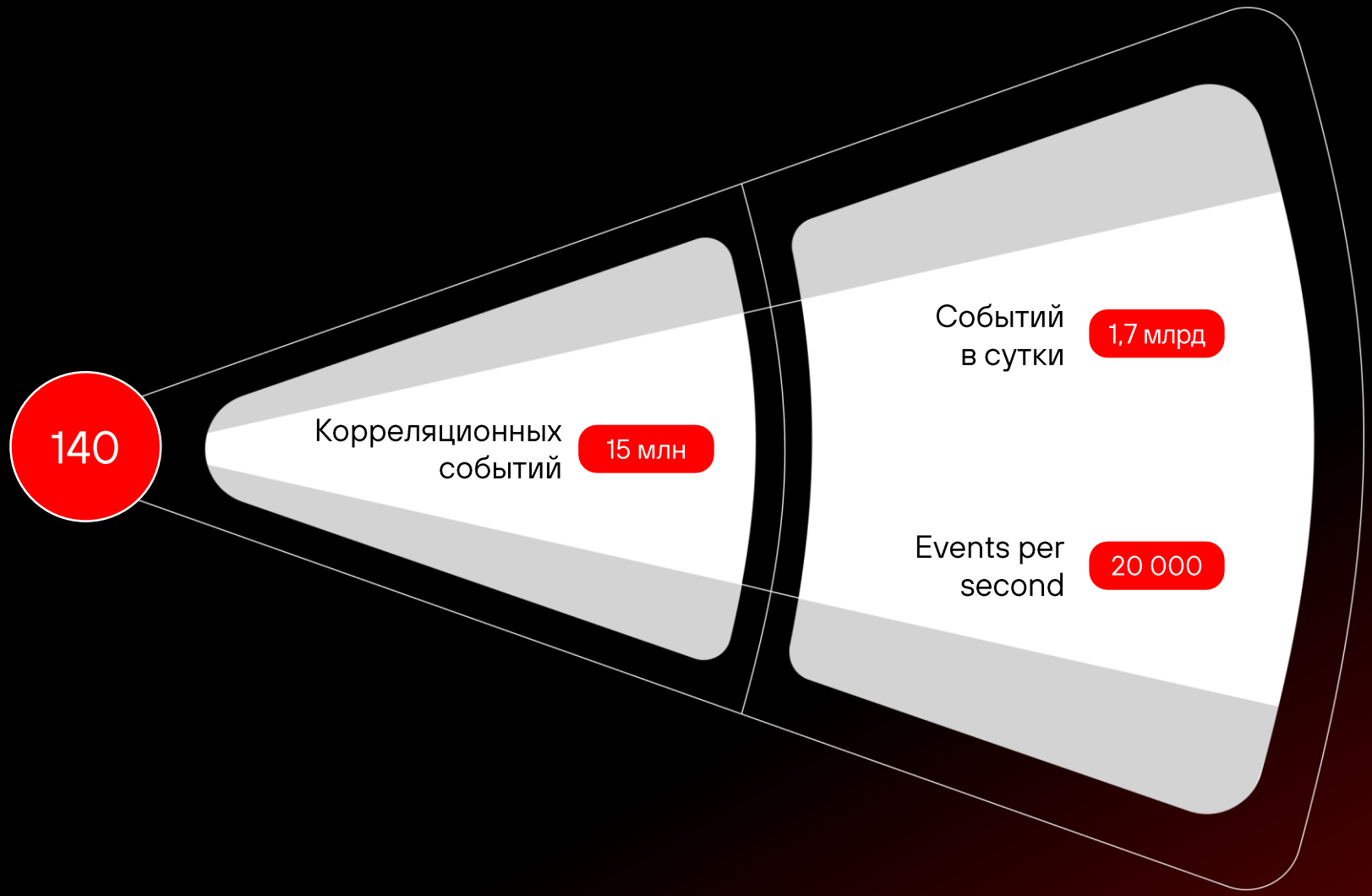
- Обнаружить
- Расследовать
- Остановить

Обнаружить

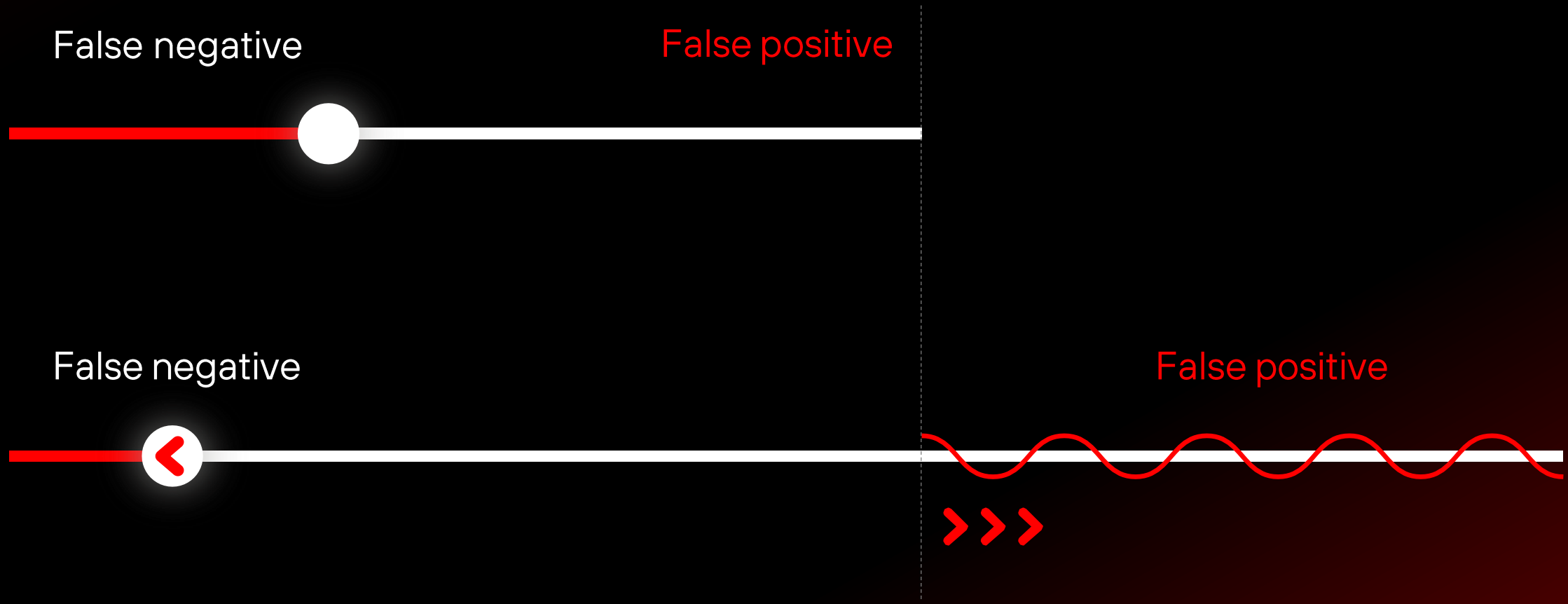

SIEM
...
NTA
Endpoint protection
Web application firewall
Sandbox
Threat Intelligence

Обнаружить

Активы: 10 000



Идеальных правил не бывает



Этапы обнаружения и реагирования на атаки

1. Анализ срабатываний СЗИ
2. Поиск связей, объединение в активности
3. Выявление ложноположительных срабатываний
4. Обогащение и расследование
5. Принятие решения о реагировании
6. Формирование сценария реагирования
7. Постановка задач по реагированию службе ИТ и контроль за их выполнением
8. Выполнение задач по реагированию службой ИБ
9. Контроль достаточности реагирования

Ключевые возможности MaxPatrol O2

выявляет активность злоумышленников в ИТ-инфраструктуре компании

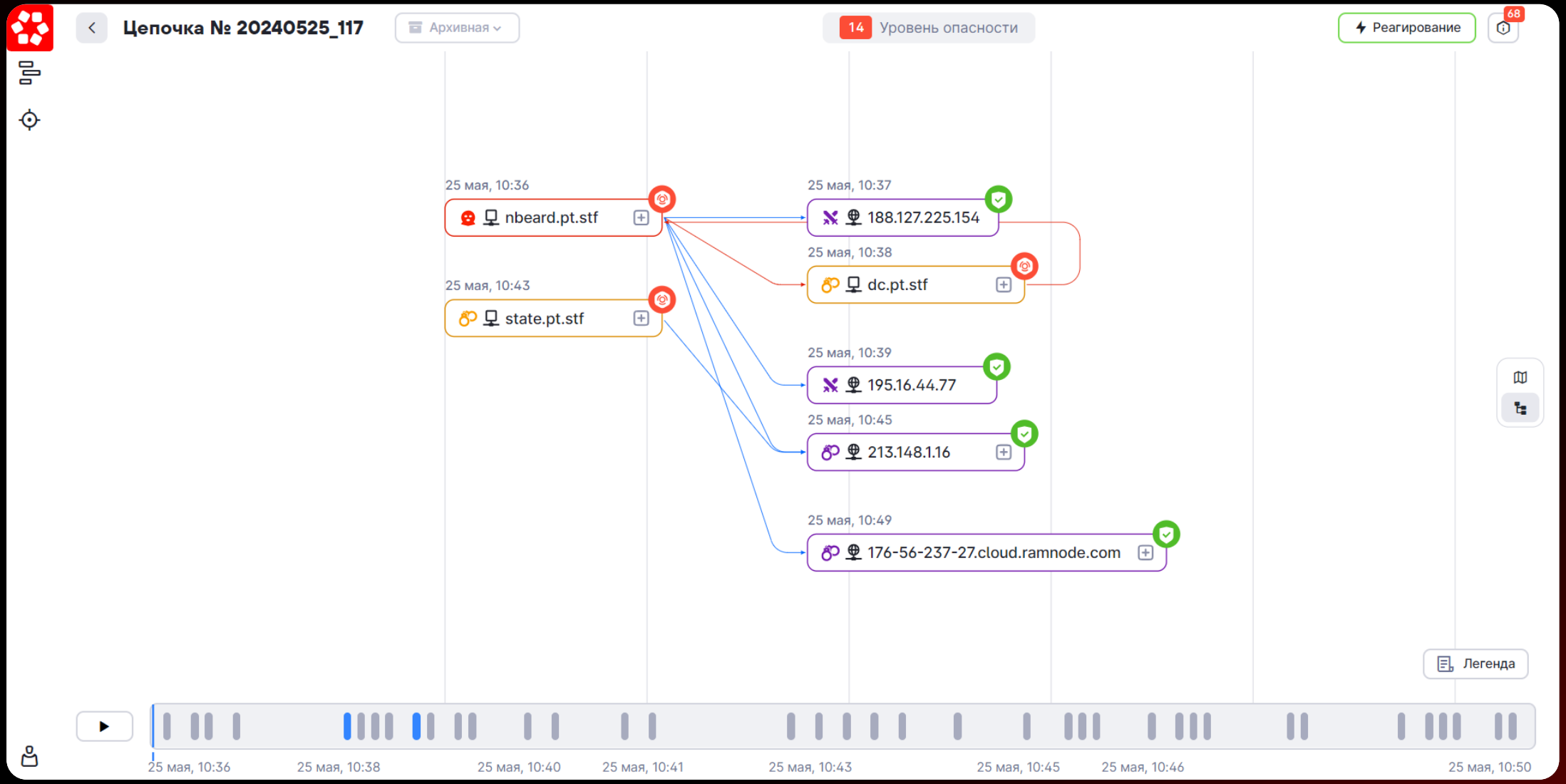
визуализирует в единый граф весь контекст атаки, необходимый эксперту для принятия решения

оценивает уровень потенциальной опасности выявленной активности и привлекает эксперта только к действительно значимым активностям

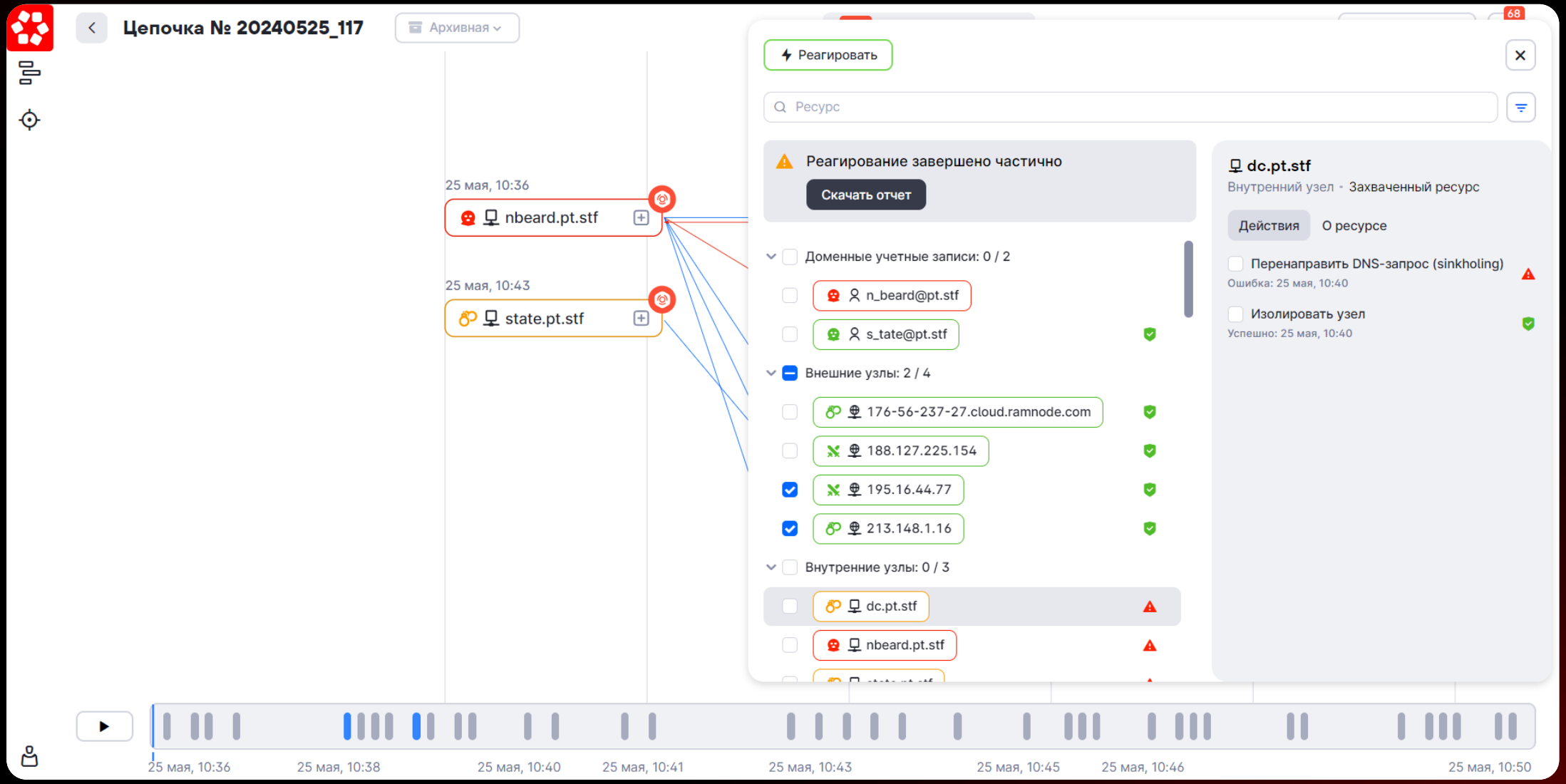
формирует и выполняет сценарий реагирования с учетом критически важных ИТ-активов и процессов организации

ретроспективно расследует путь злоумышленника в ИТ-инфраструктуре (способ проникновения, закрепление и продвижение)

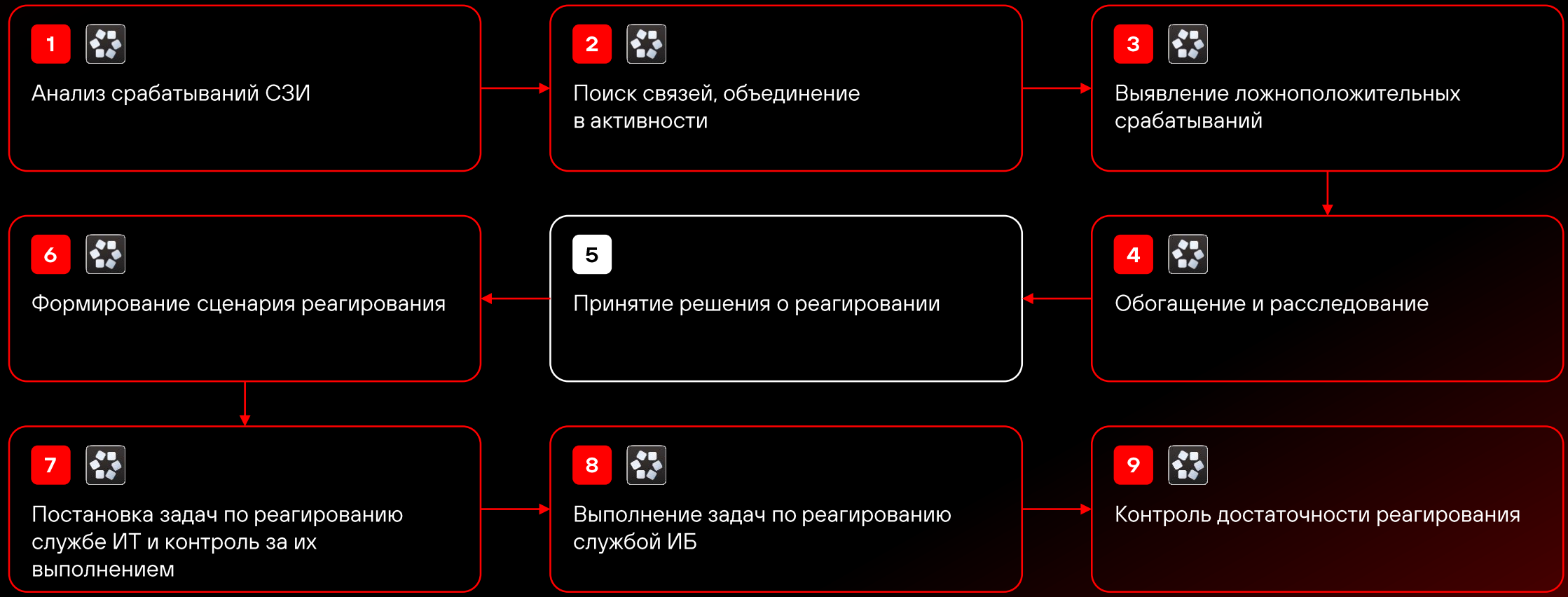
Цепочка атаки



Сценарий реагирования



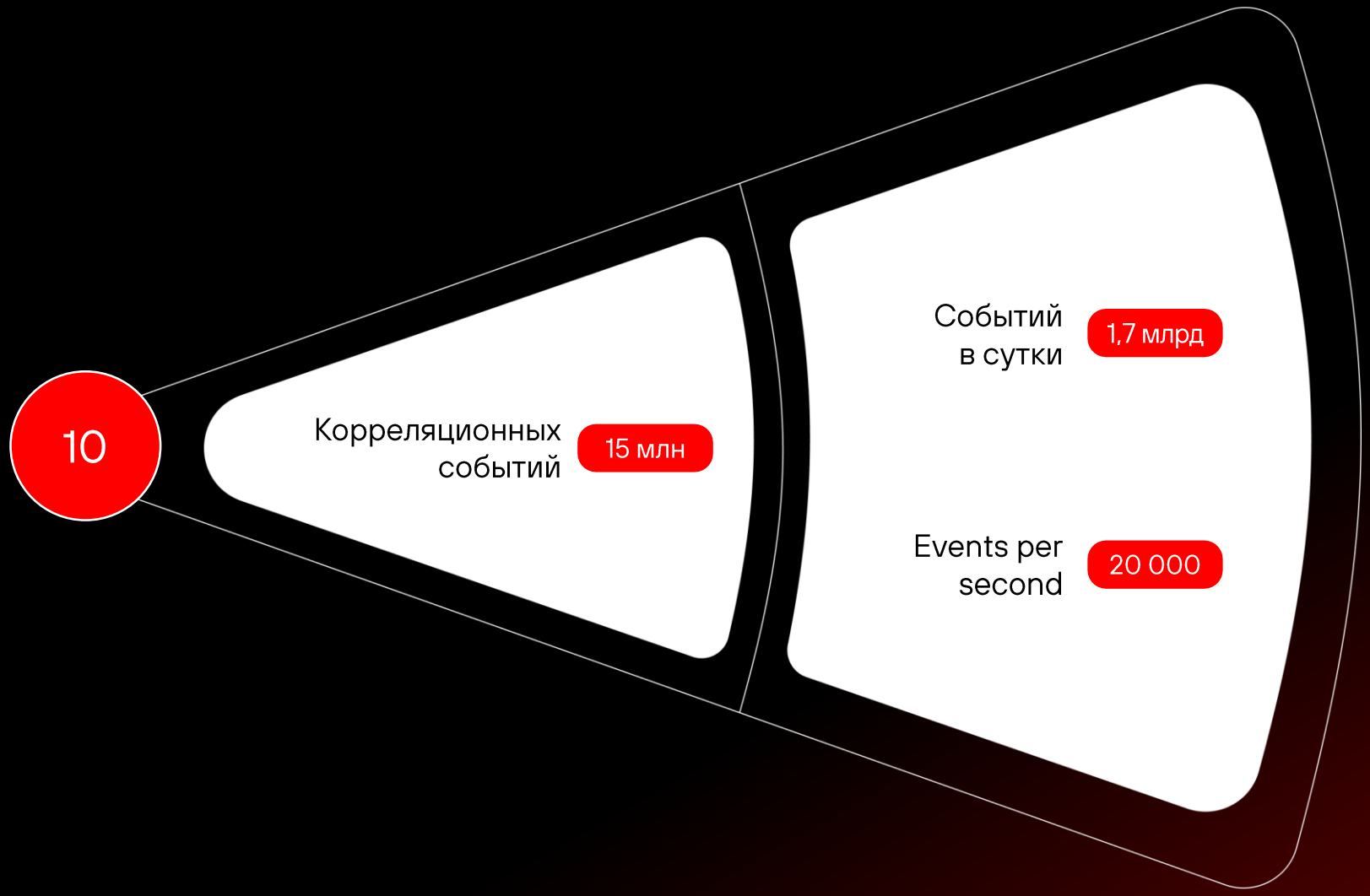
Автоматическое обнаружение и реагирование на атаки



Обнаружить

Активы: 10 000

Срабатываний в день



MaxPatrol O2 vs. 4 команды хакеров

Цель:

Защитить копию инфраструктуры Positive Technologies от атак четырех лучших команд Standoff

6 часов
противостояния хакеров и MaxPatrol O2

1 специалист
Работал с MaxPatrol O2

98 + млн
нормализованных событий

→

220 + тыс
корреляционных событий

→

1 764
цепочки в MaxPatrol O2

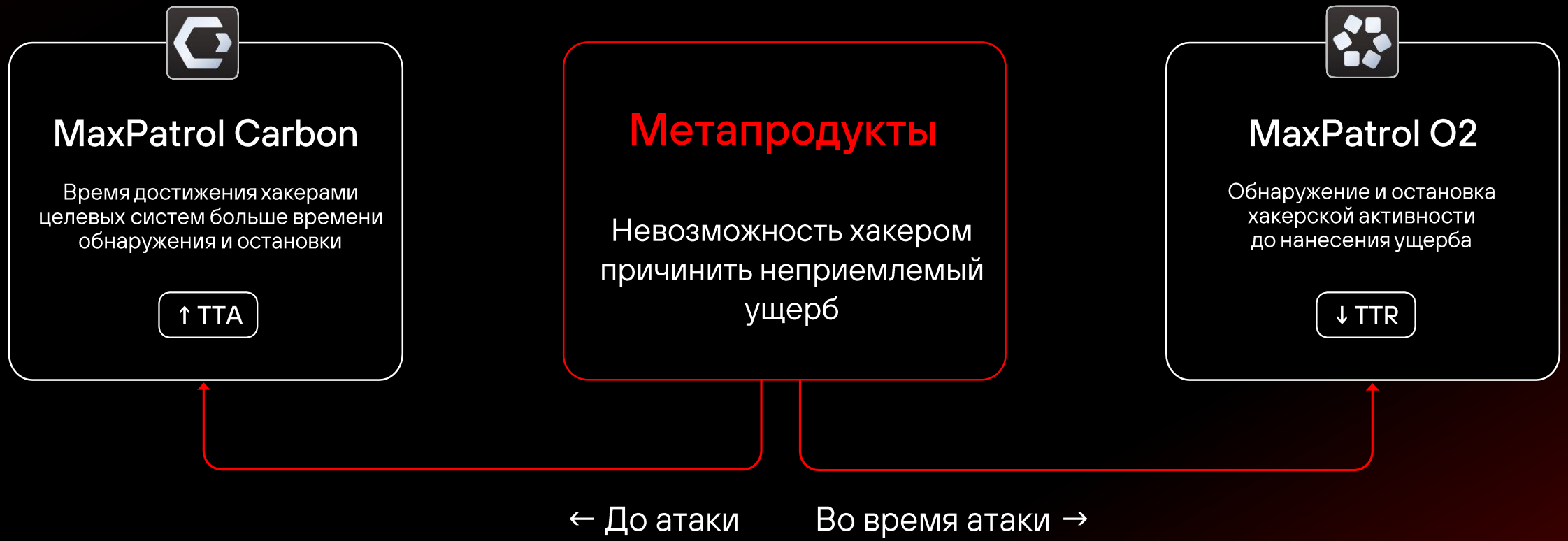
148
цепочек со статусом «Требует внимания»

Цифры по мониторингу

	Команды защитников	MaxPatrol O2	
Численность команд, чел.	Средняя: 15 Минимальная: 10 Максимальная: 25	1	Меньше в 15 раз
Время расследования	Среднее: 354 мин. Минимальное: 37 мин. Максимальное: 14 часов	2,5 мин.	Быстрее в 15 раз

MaxPatrol O2 — SOC на автопилоте

1. Уменьшает время реагирования на атаки
2. Снижает количественные требования к команде SOC
3. Снижает качественные требования к команде SOC
4. Снижает временные и интеллектуальные затраты на автоматизацию работы SOC


MaxPatrol Carbon
Время достижения хакерами целевых систем больше времени обнаружения и остановки
↑ TTA
Метапродукты
Невозможность хакером причинить неприемлемый ущерб
MaxPatrol O2
Обнаружение и остановка хакерской активности до нанесения ущерба
↓ TTR
← До атаки
Во время атаки →

MaxPatrol Carbon

MaxPatrol O2

avazhenina@ptsecurity.com