

MaxPatrol O2

Автопилот результативной
кибербезопасности



Текущая ситуация в противодействии кибератакам



Мониторинг ИТ-инфраструктуры

3



Количество активов: 10 000

Event/day

2 МЛРД

Сработок СЗИ

10-60 тыс.

Инцидентов

10-100

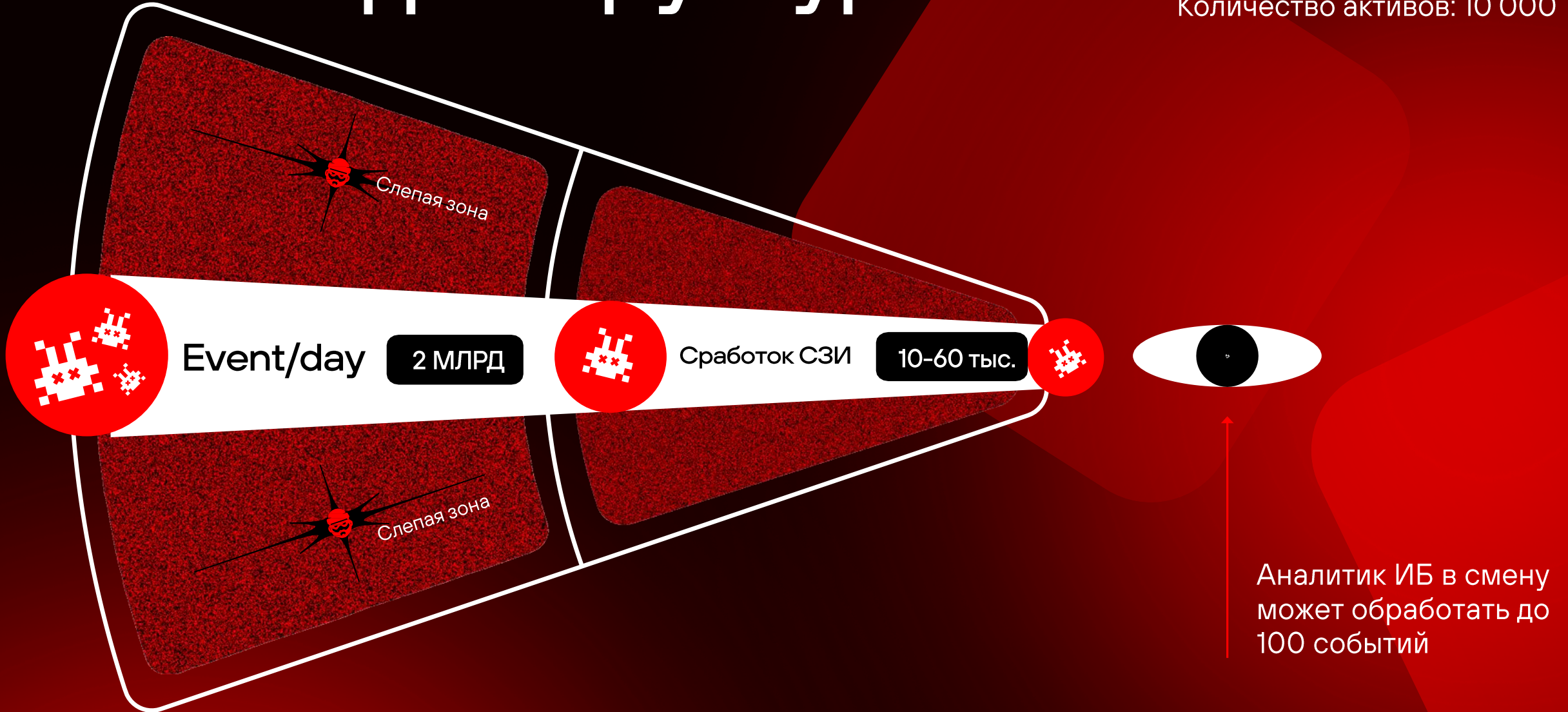
Конверсия:
600 сработок → 1 инцидент

Мониторинг ИТ-инфраструктуры

4



Количество активов: 10 000



Текущая ситуация в противодействии кибератакам

5



Нехватка специалистов
и опыта

30+ тыс.

нехватка специалистов по
информационной
безопасности в РФ

Неоптимальное использование
человеческих ресурсов

>90%

времени тратит
аналитик на обработку
false positive сработок

Недостаточное состояние
защищенности ИТ-
инфраструктуры

3,2 шага

среднее количество шагов,
необходимых хакерам для
достижения критичных активов

Как обеспечить киберустойчивость?

ЗАДАЧА

Время обнаружения и реагирования на активность злоумышленников должно быть меньше времени реализации критичных рисков ($TTR < TTA$)

РЕШЕНИЕ

УВЕЛИЧИВАТЬ ВРЕМЯ РЕАЛИЗАЦИИ АТАКИ (TTA)

1

- повышение защищенности инфраструктуры (hardening)
- исключение нелегитимных путей
- удлинение легитимных путей до реализации критичных рисков

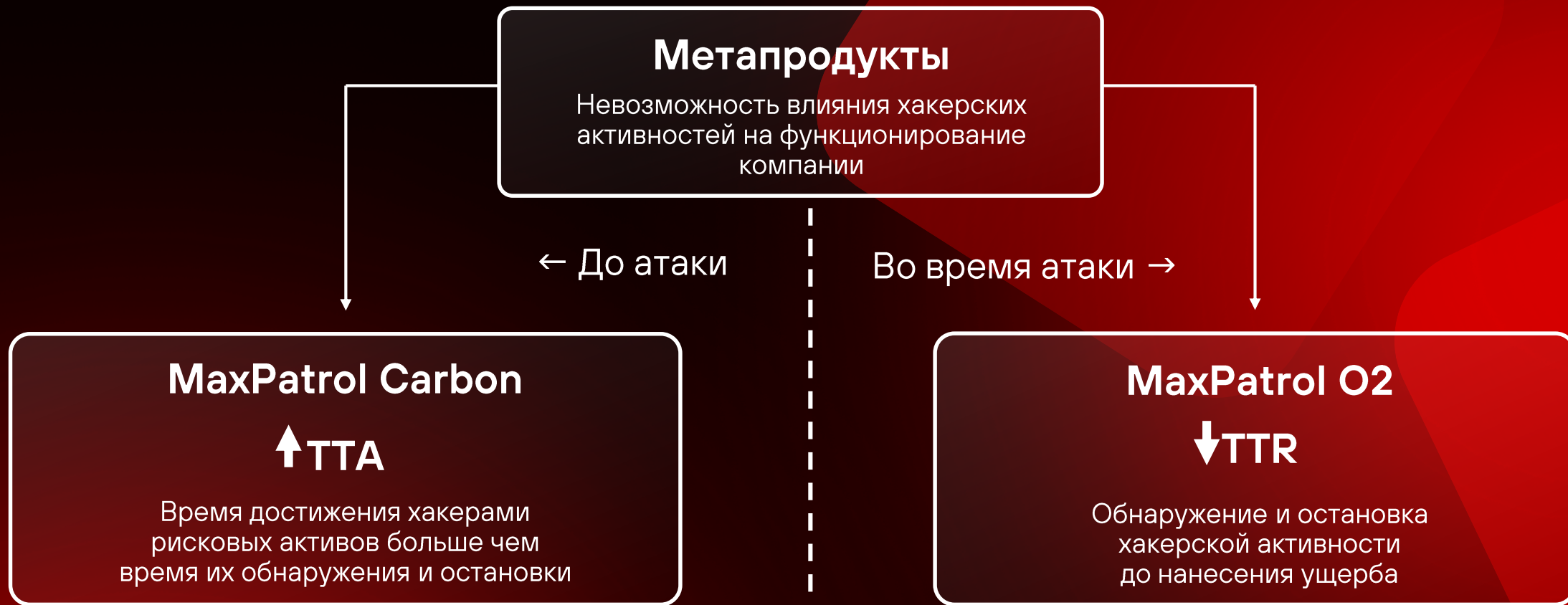
УМЕНЬШАТЬ ВРЕМЯ РЕАГИРОВАНИЯ (TTR)

2

- повышение «видимости» путей до критичных активов
- автоматический сбор информации, необходимой для принятия решений
- автоматическая генерация
- и единовременное выполнение сценария реагирования

Метапродукты для обеспечения киберустойчивости

7



Ключевые возможности MaxPatrol O2

1

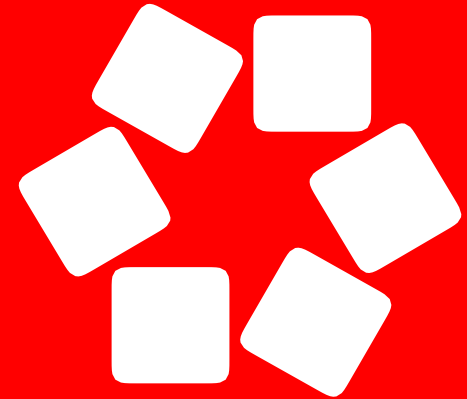
Обнаруживает злоумышленника и определяет, до каких ресурсов ему удалось добраться

2

Расследует путь продвижения злоумышленника в ИТ-инфраструктуре

3

Реагирует на атаку до того, как организации будет нанесен непоправимый ущерб

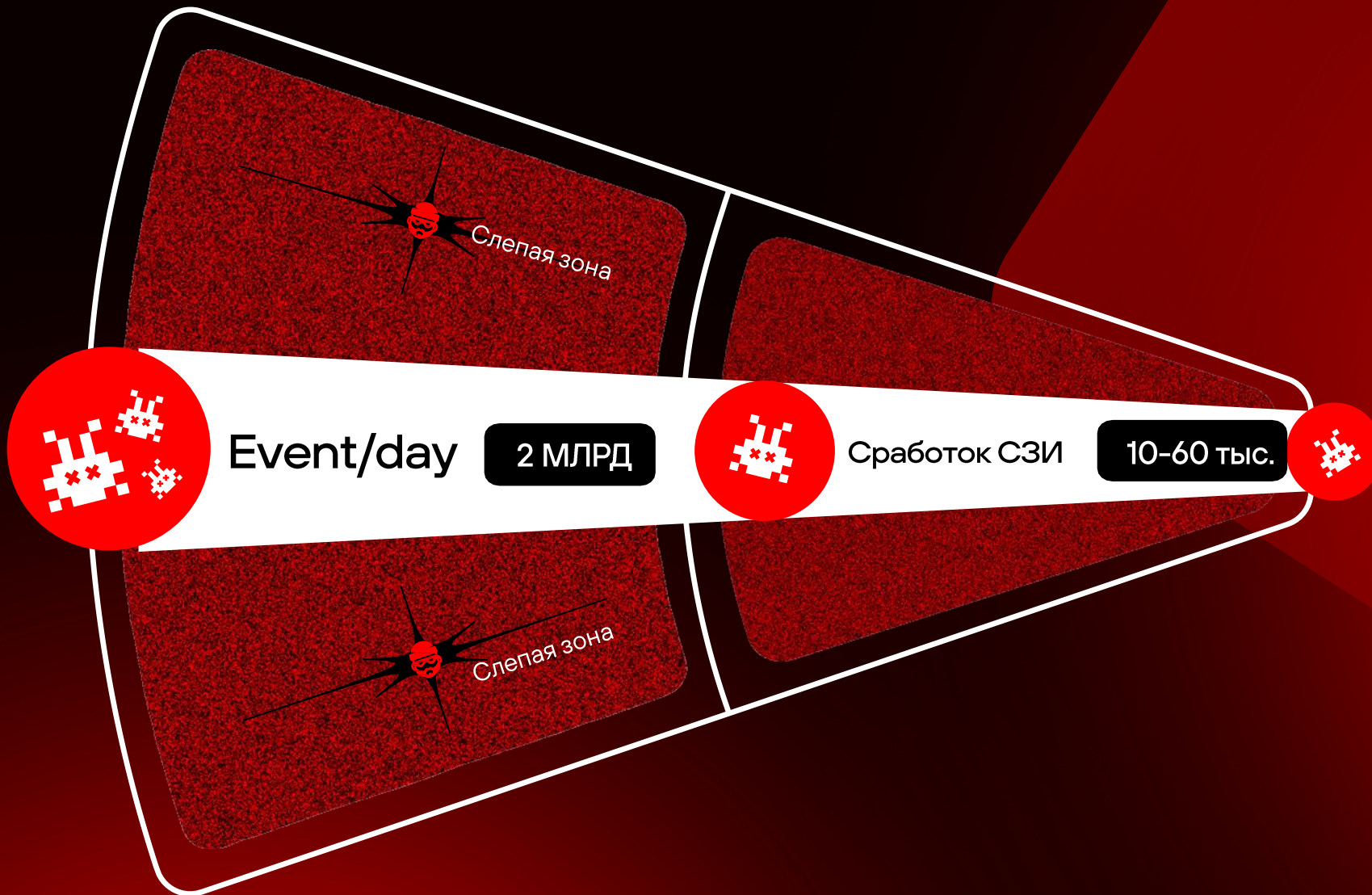


Поток событий ИБ

9



Количество активов: 10 000



Поток событий ИБ

10



Количество активов: 10 000

Event/day

2 МЛРД

Сработок СЗИ

10-60 тыс.



Цепочек

20

Проверка на Standoff

→ Цель

Подтверждение эффективности работы MaxPatrol O2

→ Решение

Мониторинг всей инфраструктуры Standoff (1 500 активов) средствами MaxPatrol O2

→ Результат

- 331 цепочка в «Требуется внимание» против 2,2 млрд корреляционных событий в SIEM
- До 350 корреляционных и нормализованных событий объединены в одну цепочку. Время расследования такой цепочки blue team – 8 часов

→ Подтверждение

Результаты работы MaxPatrol O2 подтверждены путем сравнения с отчетами red teams

Проверка эффективности «боем» в инфраструктуре заказчика

12



→ Цель

Подтверждение эффективности работы MaxPatrol O2

→ Решение

Проведение киберучений двумя командами: классический подход и используя MaxPatrol O2
Red team HE Positive Technologies

→ Результат

- MaxPatrol O2 обнаружил активность red team
- Выявлено 2 факта нелегитимной деятельности сотрудников компании
- В 8 раз меньше сработок, требующих внимания, и в 5 раз меньше время, затрачиваемое на их анализ

→ Подтверждение

Результаты работы MaxPatrol O2 подтверждены отчетом red team

Защита крупной организации

→ Цель

Обеспечение защиты от хакерских атак ИТ-инфраструктуры организации

→ Решение

Создание ЦПК с использованием MaxPatrol O2

→ Результат

- За 1 месяц работы выявлена активность реальной хакерской группировки.
- В ходе расследования установлено, что данная группировка присутствует в ИТ-инфраструктуре компании более 1 года

→ Подтверждение

Верификация результатов работы MaxPatrol O2 командой ESC Positive Technologies

MaxPatrol O2 на Играх будущего

→ Цель

Обеспечение защита мероприятий международного уровня от хакерских атак

→ Решение

Использование MaxPatrol O2 в качестве «второго пилота» ЦПК

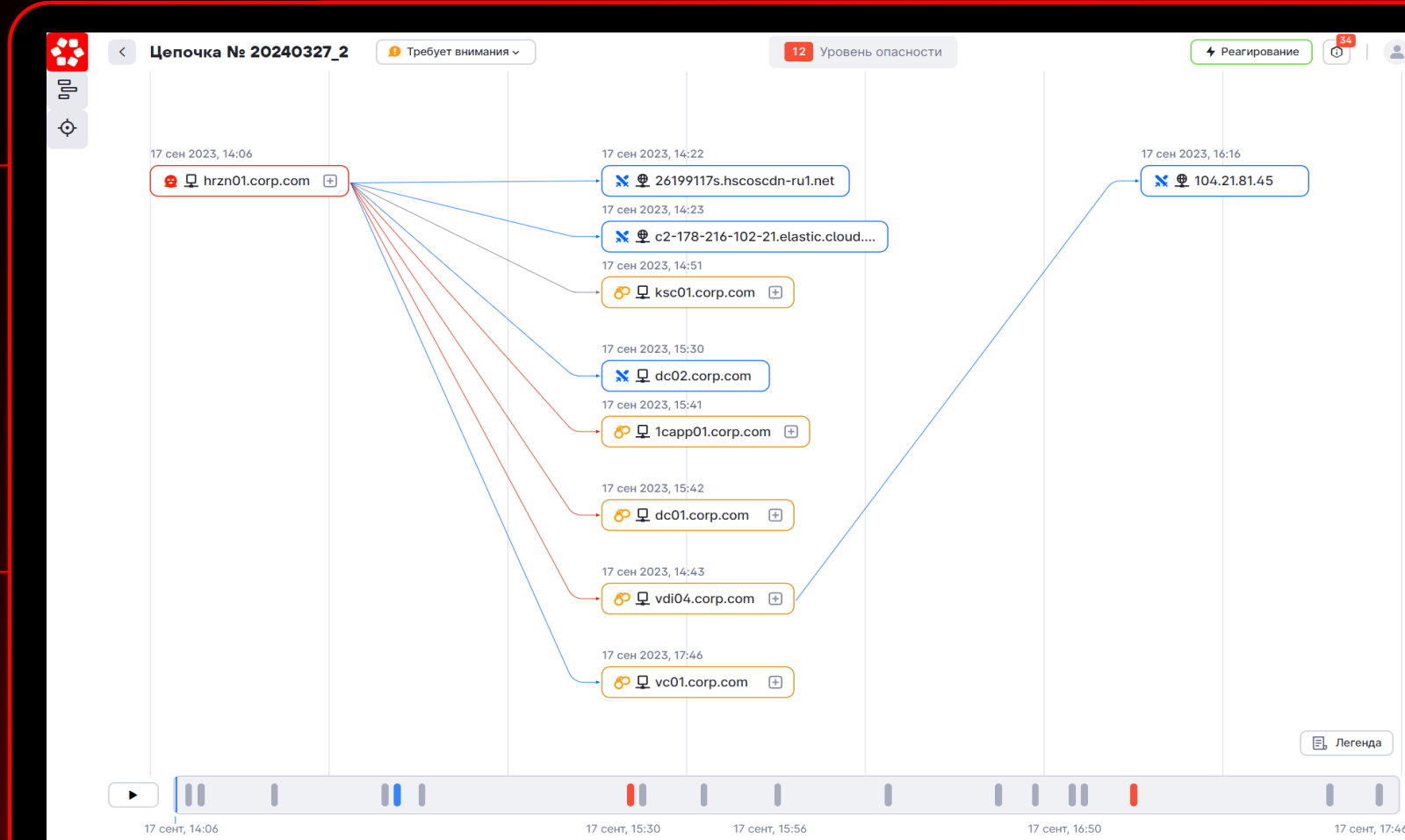
→ Результат

	Команда ЦПК	MaxPatrol O2
Количество сработок, требующих внимания в день	109-517	2-4
Численность команды	33 человека	1 человек в смену
Время, затрачиваемое на обработку инцидентов в день	36 человеко-часов	1,5 человеко-часов

Выявление активности злоумышленников

Анализирует данные от сенсоров Positive Technologies

Объединяет отдельные сработки сенсоров в цепочки активности с учетом причинно-следственных связей

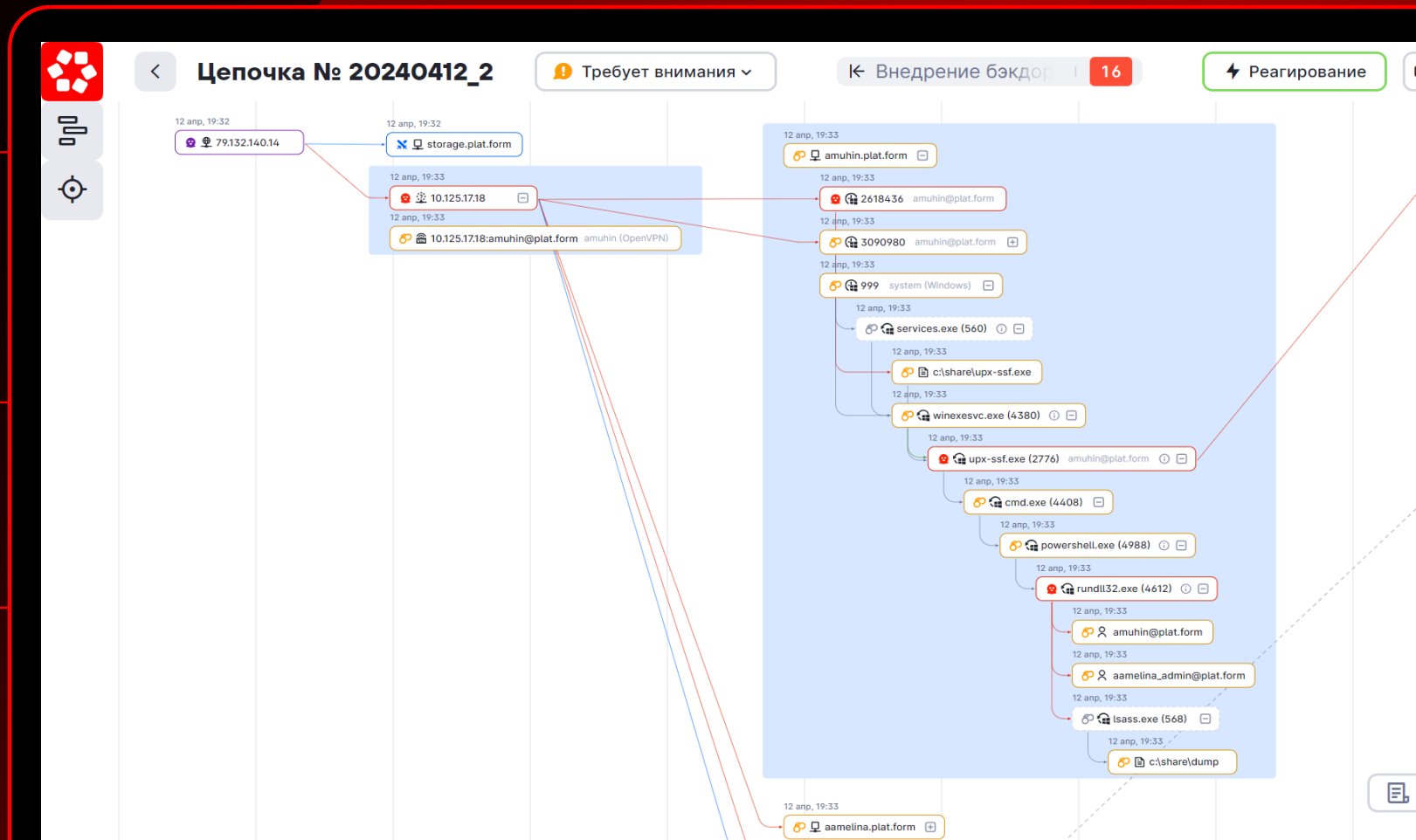


Автоматизация расследования

Проводит ретроспективный анализ продвижения злоумышленника

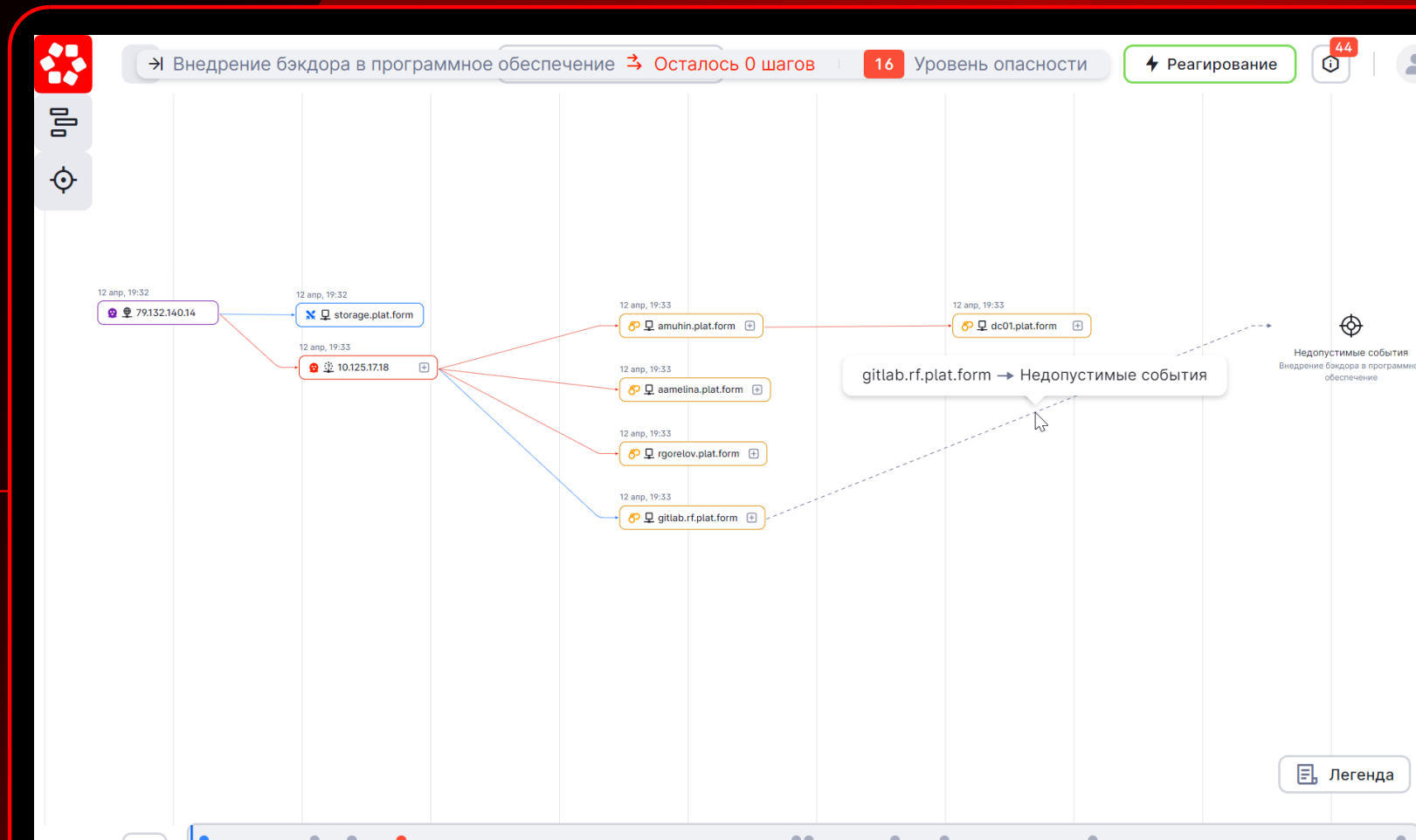
Определяет способ проникновения в инфраструктуру, закрепления и продвижения

Восстанавливает хронологию атаки. Предоставляет весь контекст, необходимый для принятия решения



Оценка достижимости критичных активов

Знает, как злоумышленник сможет добраться до критичных активов, а также количество шагов, которые ему потребуется совершить



Оценка уровня потенциальной опасности

Рассчитывает потенциальную опасность активности на основе 10+ параметров: наличие паттернов атак, используемые тактики, захват критичных узлов, индикаторы компрометации и другие

Переводит цепочку атаки в статус «Требуется внимания» и привлекает эксперта только к действительно значимым активностям

Цепочки

Любой параметр ресурса или идентификатор события

Собирается

Требуется внимания

Ложное срабатывание

Архивная

Уровень опасности

Цепочка № 20240327_8

21 ноя 2023, 16:07 → 21 ноя 2023, 19:04

30 событий

109 ресурсов

20

Уровень опасности

Цепочка № 20240327_10

22 ноя 2023, 14:18 → 22 ноя 2023, 19:21

343 события

508 ресурсов

18

Уровень опасности

Цепочка № 20240327_14

22 ноя 2023, 19:22 → 23 ноя 2023, 15:23

42 события

177 ресурсов

14

Уровень опасности

Цепочка № 20240327_2

17 сен 2023, 14:06 → 17 сен 2023, 17:46

34 события

114 ресурсов

12

Уровень опасности

Цепочка № 20240327_6

16 ноя 2023, 19:29 → 16 ноя 2023, 19:29

1 903 события

453 ресурса

11

Уровень опасности

Цепочка № 20240327_7

21 ноя 2023, 15:25 → 21 ноя 2023, 15:56

41 событие

80 ресурсов

4

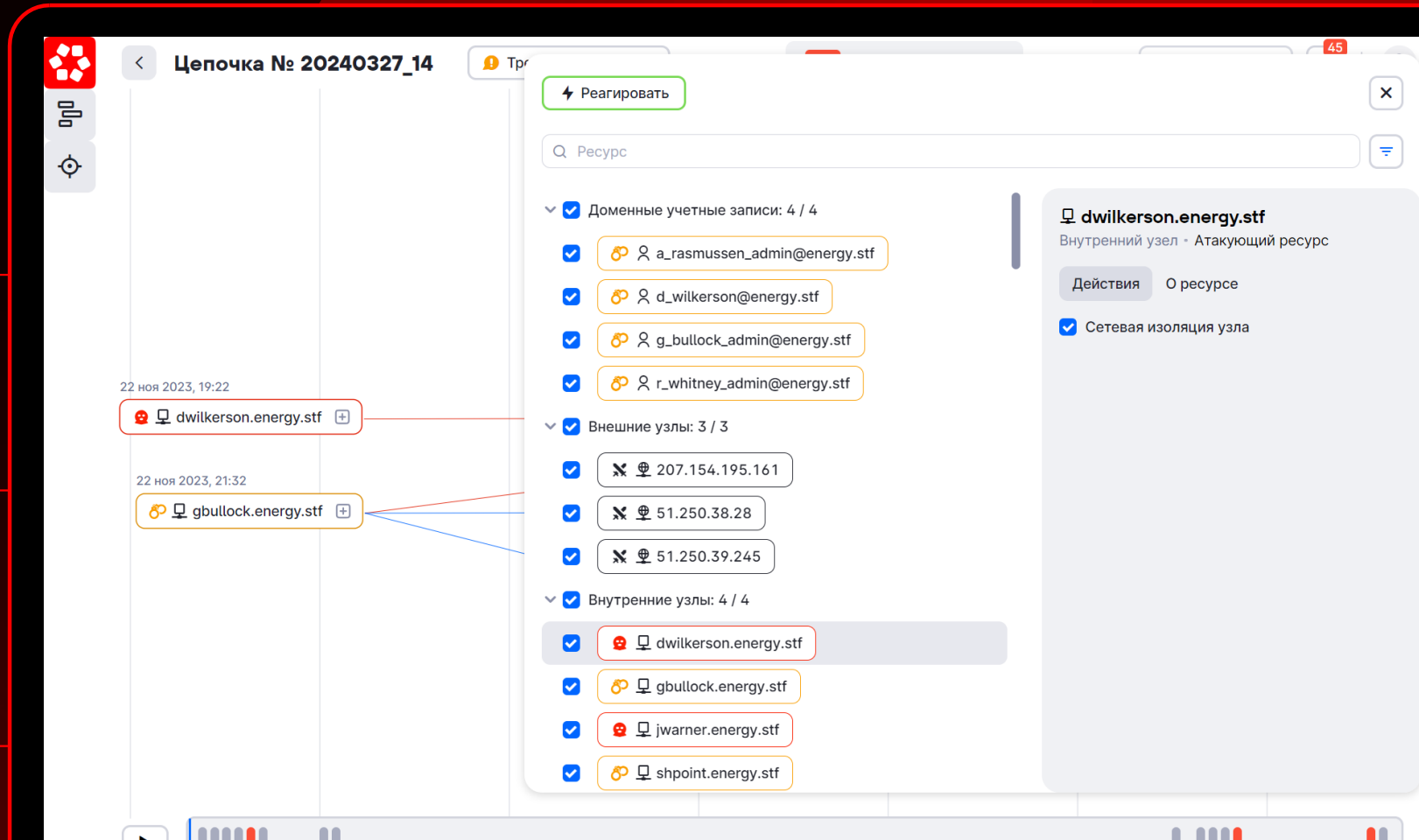
Уровень опасности

Остановка злоумышленника

Динамически составляет сценарий реагирования для любых типов атак

Учитывает ограничение реагирования на наиболее значимые активы

Поддерживает автоматический запуск сценария реагирования или с привлечением эксперта



Эффект от внедрения MaxPatrol O2

20



Уменьшает TTR

Выделение действительно значимых активностей из общего числа инцидентов, их автоматическое расследование и генерация сценария реагирования

Снижает качественные требования к команде SOC

Осуществление всей сложной, трудоемкой аналитики по атаке. Специалистам остается только верифицировать шаги, предложенные для остановки злоумышленника

Позволяет обнаружить и своевременно остановить злоумышленников с минимальным участием людей до того, как они успеют нанести организации непоправимый ущерб

Снижает количественные требования к команде SOC

Кратное уменьшение количества сработок, требующих внимания сотрудников, повышение их информативности и снижение числа ложноположительных сработок

Снижает временные и интеллектуальные затраты на автоматизацию SOC

Исключение трудозатрат на самостоятельную автоматизацию процессов в SOC или кастомизацию иных решений

Спасибо

pt@ptsecurity.com
ptsecurity.com





Этапность внедрения MaxPatrol O2





Этапность внедрения MaxPatrol O2

