SOC на автопилоте
Как и куда едем?

Михаил Кадер

АО «Позитив Текнолоджиз»

02.04.2024

ptsecurity.com

Вопрос не в том, взломают ли вопрос в том - когда

90%

компаний взламываются от одного до пяти дней

9 из 10

жертв не замечают факт взлома

200 дней

составляет среднее время обнаружения компрометации

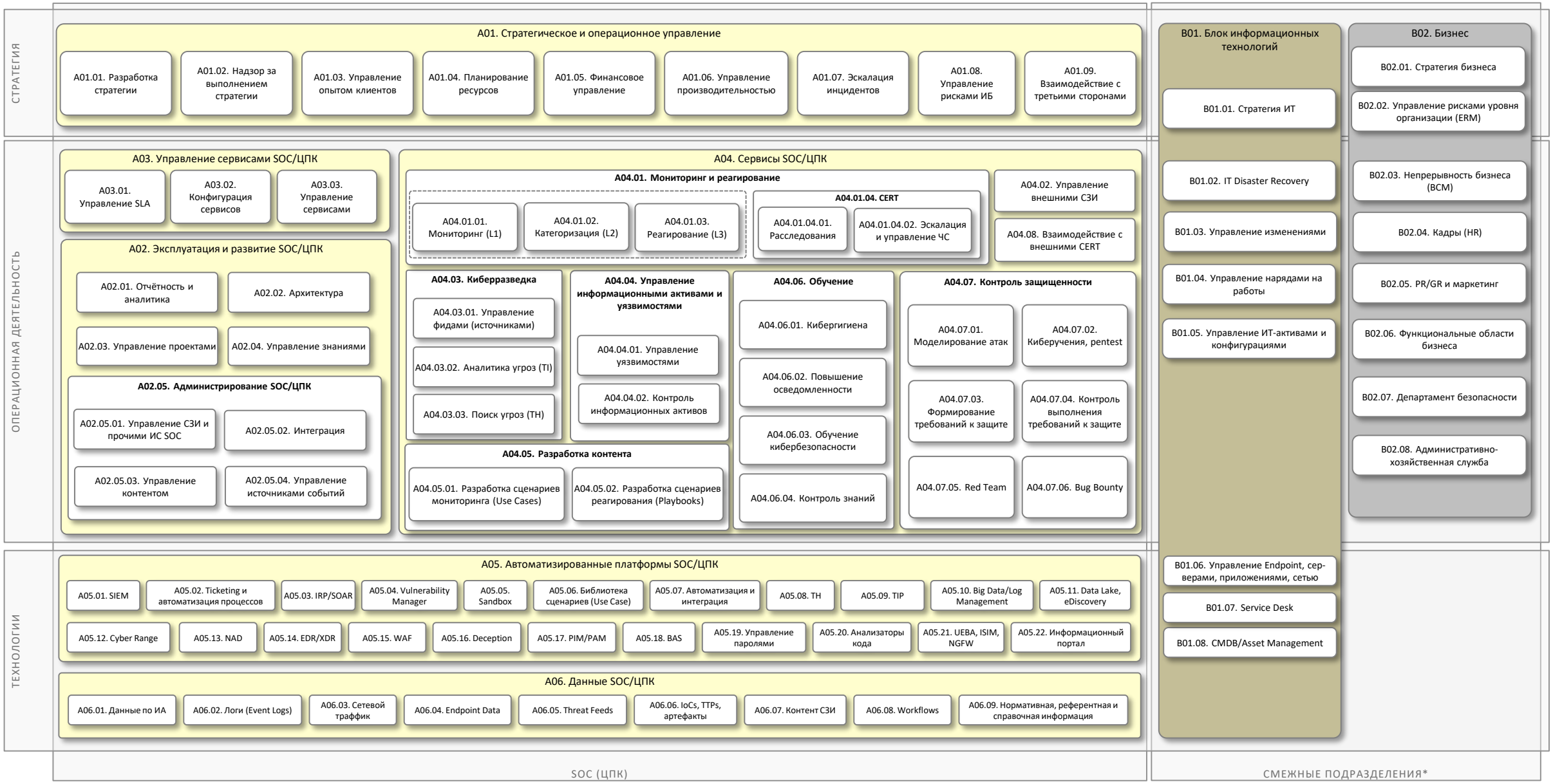
Задачи SOC

SOC

- экспертная команда, которая глубоко понимает современный ландшафт киберугроз в мире
и адаптирует систему ИБ под новые угрозы

- Предотвращает инциденты
- Выявляет целенаправленные атаки на инфраструктуру
- Снижает время обнаружения и реагирования на инцидент
- Использует средства ИБ с максимальной результативностью

Операционная модель SOC (спасибо Константину Смирнову)



Центр противодействия киберугрозам (ЦПК)

Обеспечение КиберУстойчивости предприятия

– **набор функций** (сервисов) ИБ, распределенных между внутренними и внешними **командами** (сотрудниками), **описанный через десятки процессов** стратегического, тактического и оперативного уровня и **реализованный с использованием технологий** детектирования, анализа, корреляции и реагирования для обеспечения невозможности наступления **недопустимых событий**

Формализованные и внедренные процессы и соответствующие регламенты работ специалистов ЦПК

Средства защиты, мониторинга, расследования **инцидентов**, реагирования и т.п.

Проверка полноты и качества построения ЦПК и невозможности реализации недопустимых событий

Специалисты, обладающие необходимыми знаниями и опытом и постоянно повышающие квалификацию на киберучениях, а также экспертиза внутри продуктов

Из чего состоит кибер-безопасность в компании?

Процесс №1

Решения

Программные
и аппаратные

Люди

Сотрудники ИБ-
и ИТ
подразделений

Процесс №2

Решения

Программные
и аппаратные

Люди

Сотрудники ИБ-
и ИТ
подразделений

Процесс № ...

Сколько специалистов по ИБ нужно для мониторинга

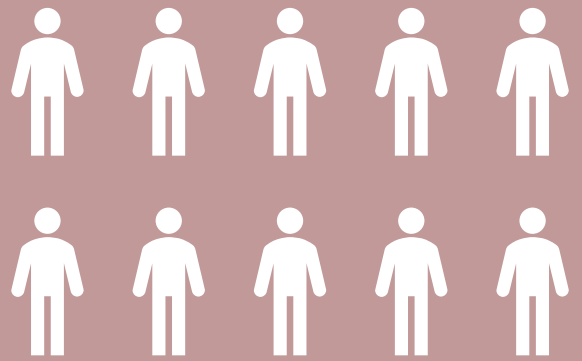
10 000 активов, 30 000 EPS

>

Смотрит только наиболее критически опасные инциденты

>

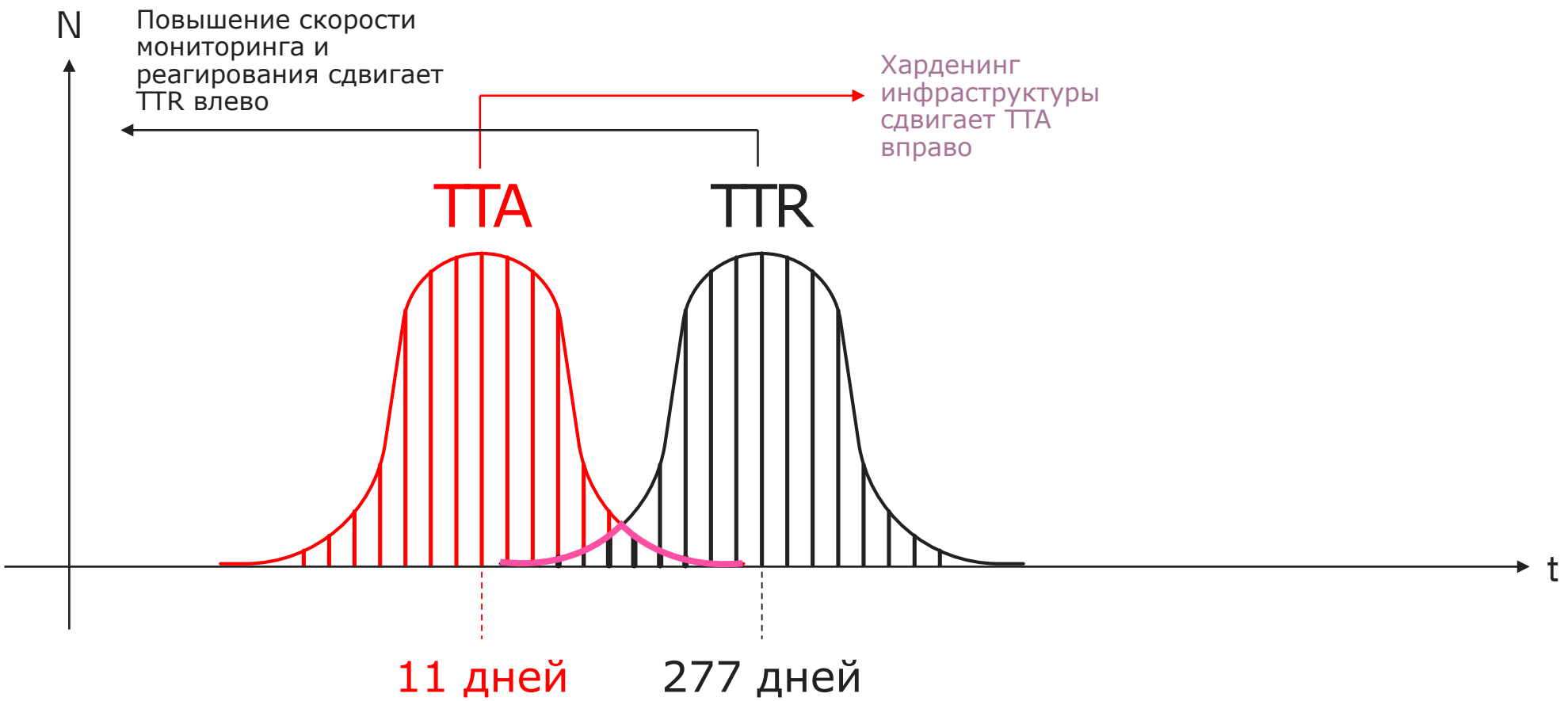
Смотрят все инциденты



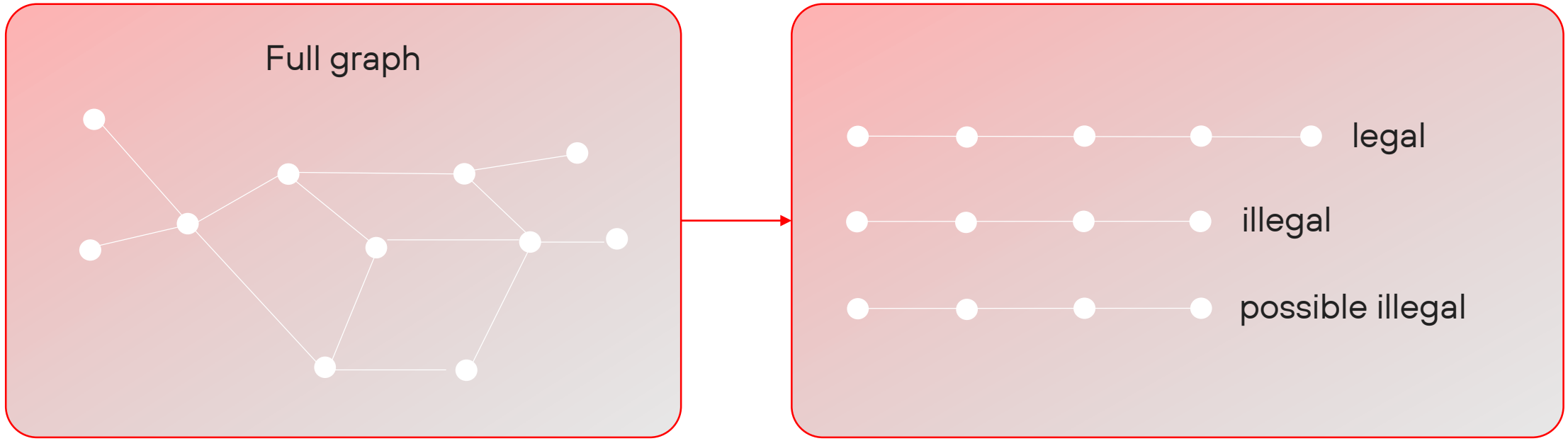
>

Смотрят все сработки СЗИ

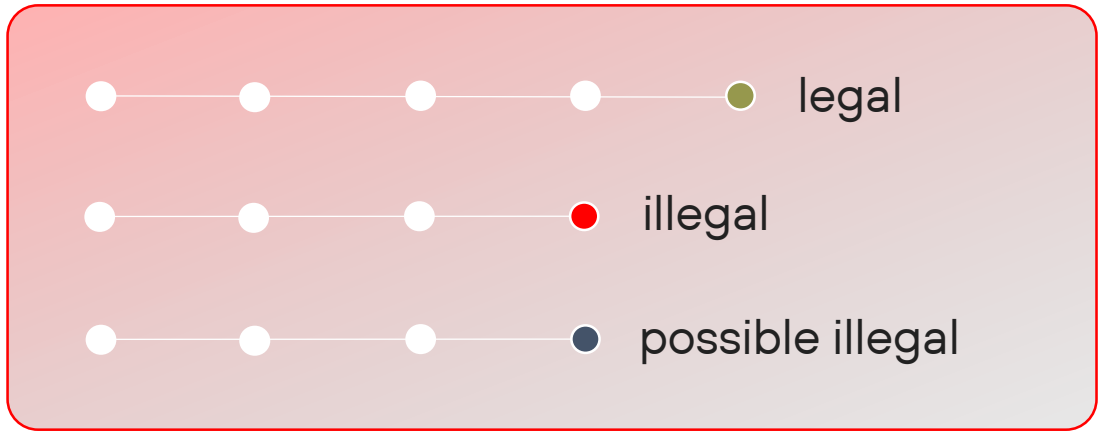
Атаки успешны, когда TTA < TTR



Анализ маршрутов реализации недопустимых событий



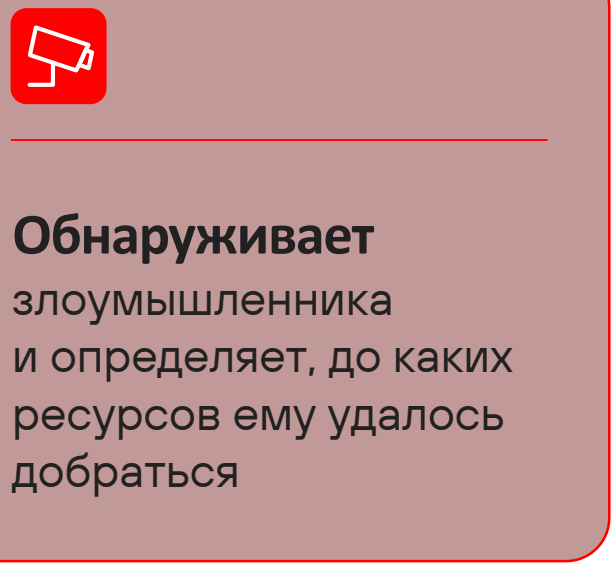
Анализ маршрутов и формирование рекомендаций



Рекомендации

- Устранить уязвимость CVE-... на узле «host»
- Добавить второй фактор аутентификации для сервиса «Portal»
- Настроить сбор событий в SIEM с узла «host»
- Завести траффик в МСЭ между узлами «host — host»

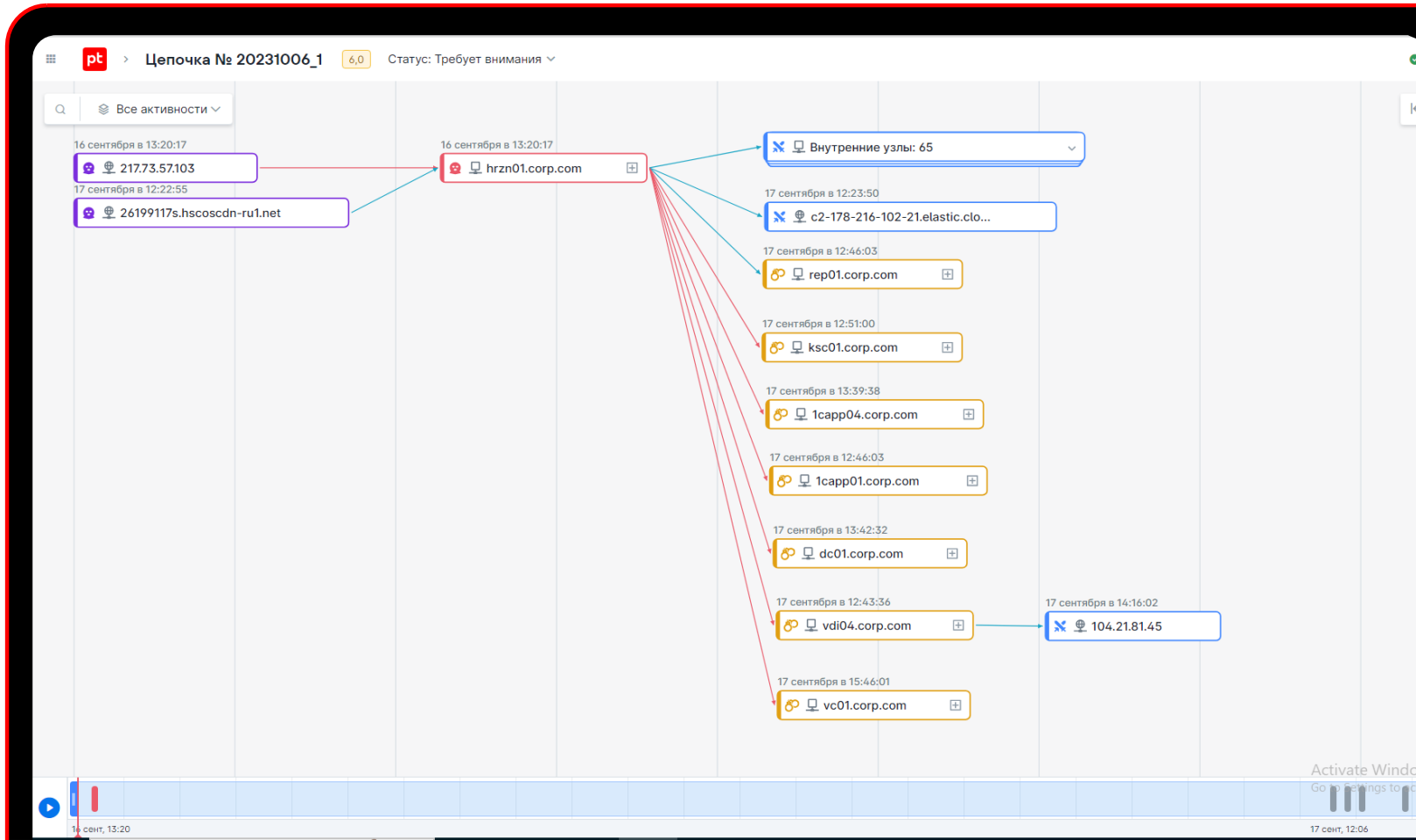
Автопилот для результативной кибербезопасности



Выявление активности злоумышленников

Анализировать данные от сенсоров

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

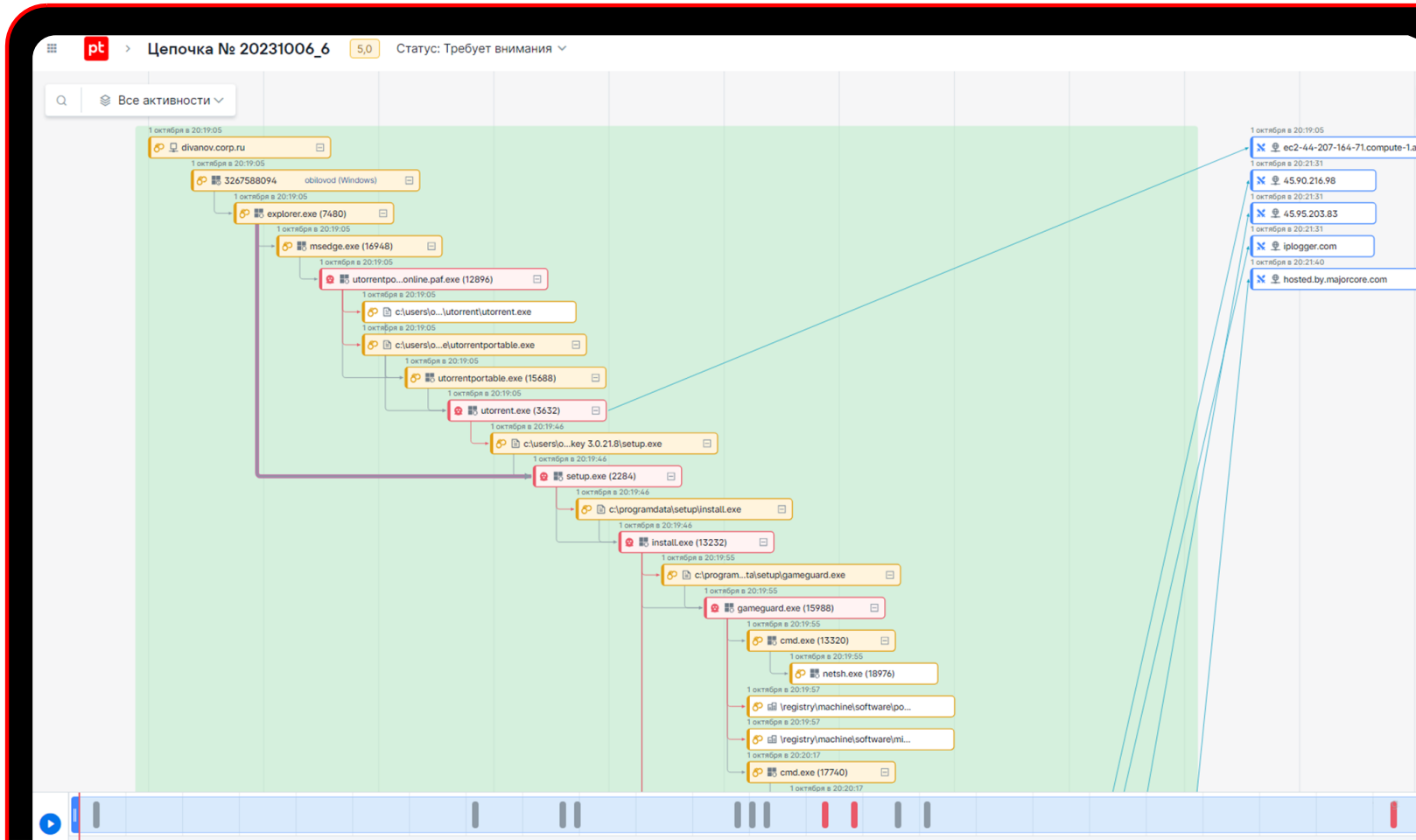


Автоматизация расследования

Проводить ретроспективный анализ продвижения злоумышленника

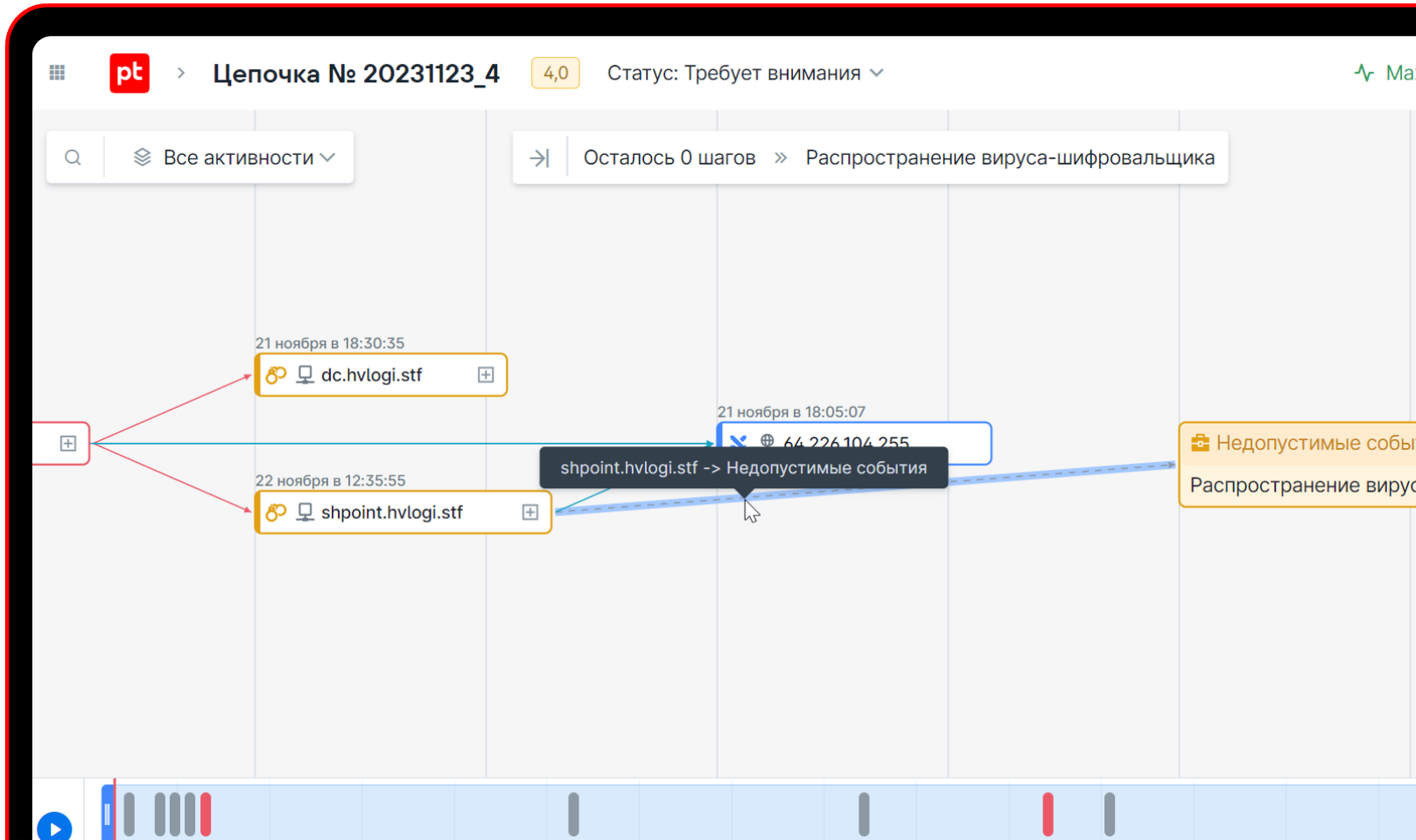
Определять способ проникновения в инфраструктуру, закрепления и продвижения

Восстанавливать хронологию атаки



Оценка достижимости критичных активов

Знать, как злоумышленник
может добраться
до критичных активов,
а также количество шагов,
которые ему потребуется
совершить



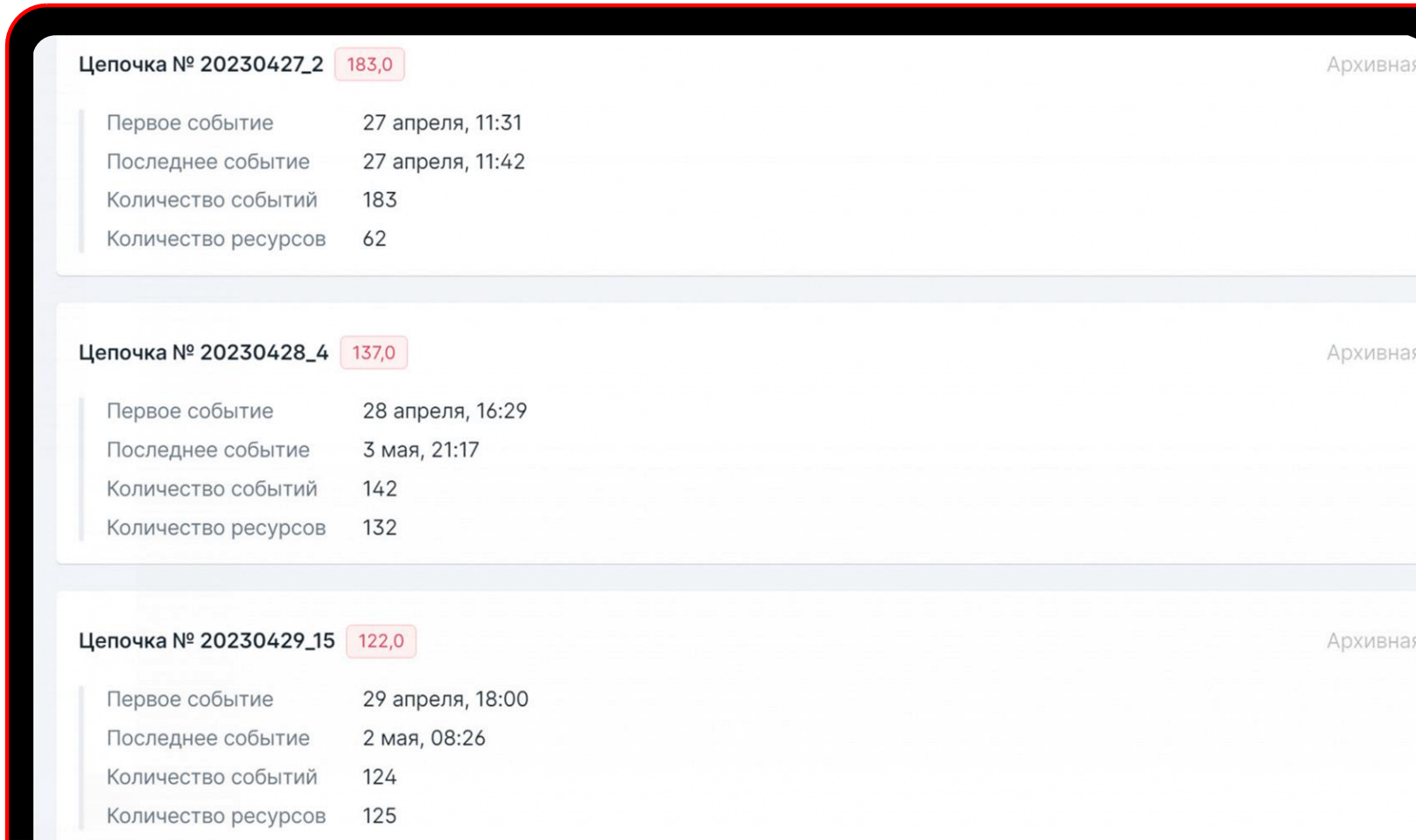
Оценка уровня потенциальной опасности

>

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

>

Переводить цепочку атаки в статус «Требует внимания» и привлекать эксперта только к действительно значимым активностям



Остановка злоумышленника

>

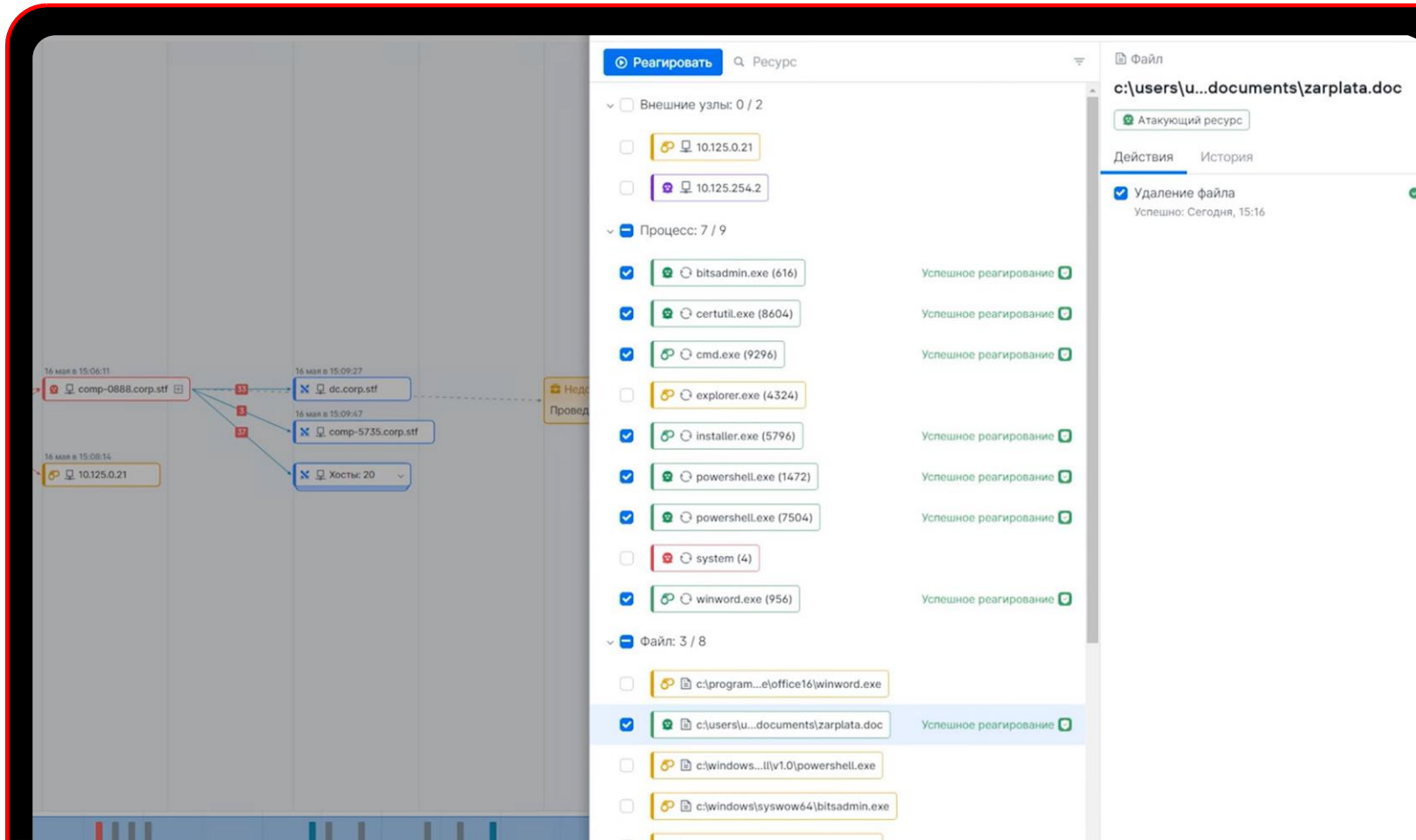
Динамически составить сценарий реагирования для любых типов атак

>

Учитывать ограничения реагирования на наиболее значимые активы

>

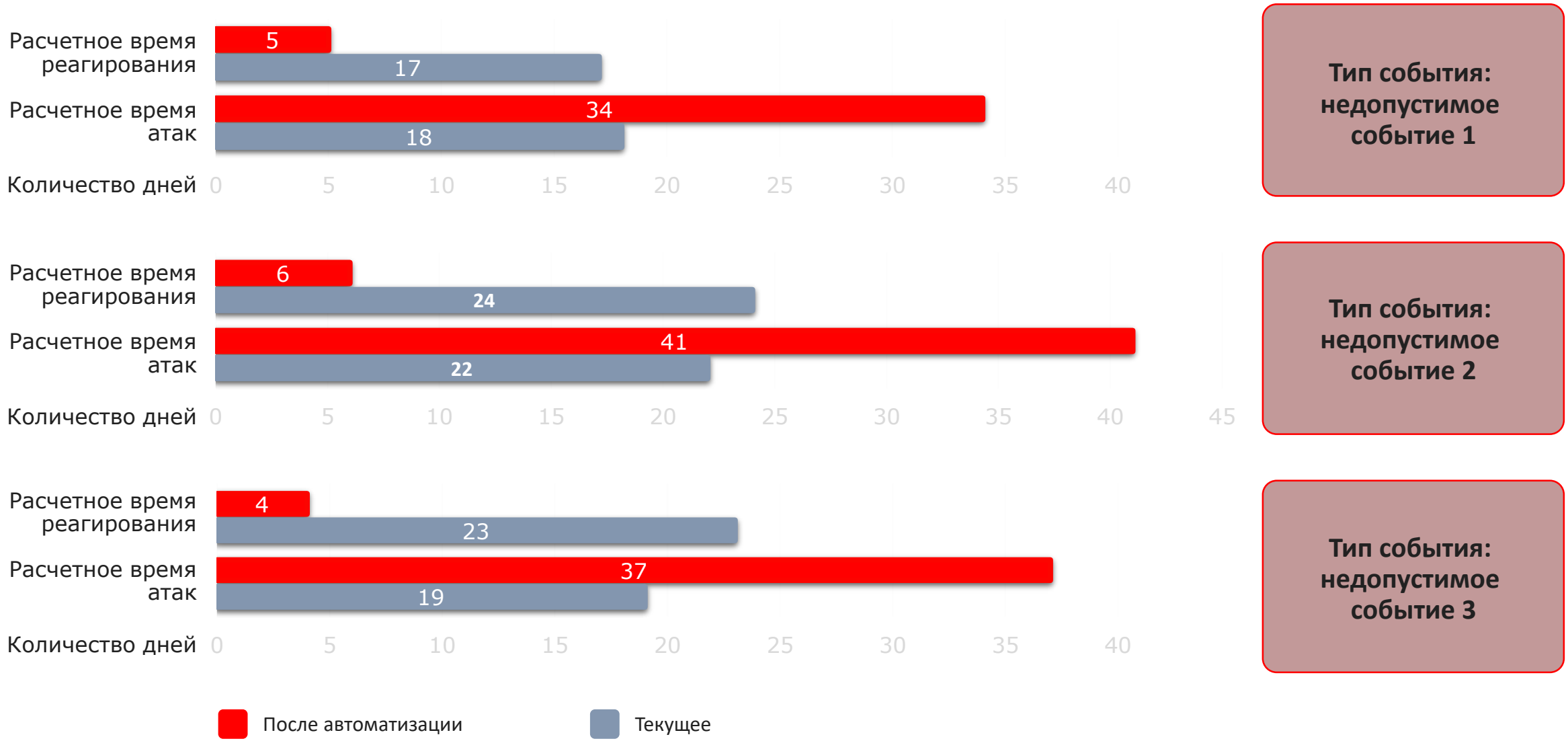
Поддерживать автоматический запуск сценария реагирования или с привлечением эксперта



Результаты киберучений – на практике

	Классический подход	Как меняется ситуация с автоматизацией	
Сработок, требующих внимания	432	3	
Время верификации и расследования	64 часа	30 мин.	
Коэффициент обработанных сработок	83 %	100 %	
Время реагирования		<1 мин.	10 сек. Формирование сценария 30 сек. Выполнение

Результаты расчетных внедрений



Тип события: недопустимое событие 1

Тип события: недопустимое событие 2

Тип события: недопустимое событие 3

- Автоматизация – наше все
- Недопустимые события - путь к повышению эффективности автоматизации
- Практика – критерий истины ☺

Спасибо
за внимание

ptsecurity.com