

SOC на автопилоте Как и куда едем?

Михаил Кадер

АО «Позитив Текнолоджиз»

02.04.2024

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

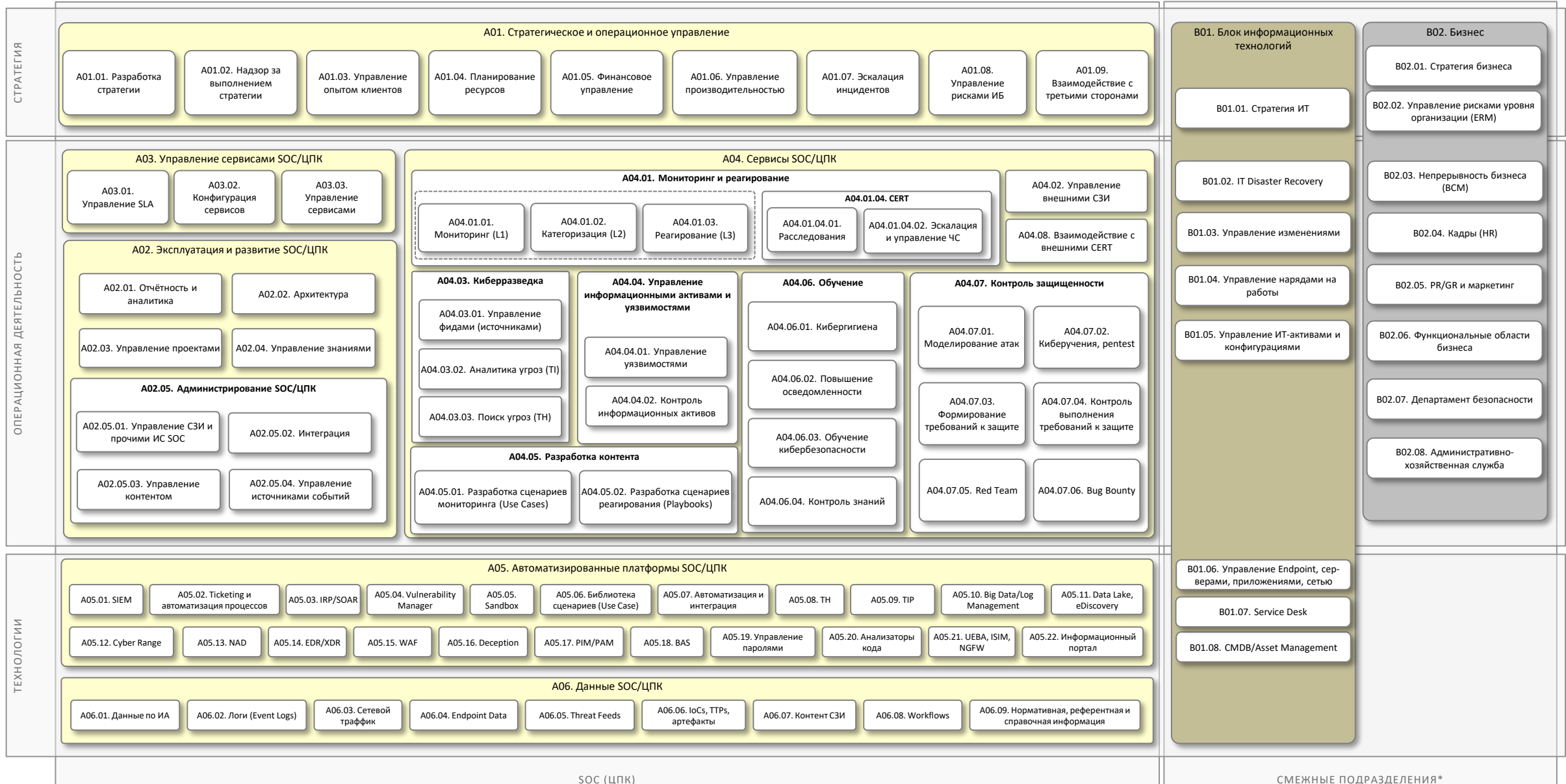
Предотвращает инциденты

Выявляет целенаправленные атаки на инфраструктуру

Снижает время обнаружения и реагирования на инцидент

Использует средства ИБ с максимальной результативностью

Операционная модель SOC (спасибо Константину Смирнову)



SOC (ЦПК)

СМЕЖНЫЕ ПОДРАЗДЕЛЕНИЯ*

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

Проверка полноты и качества построения ЦПК и невозможности реализации недопустимых событий



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

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

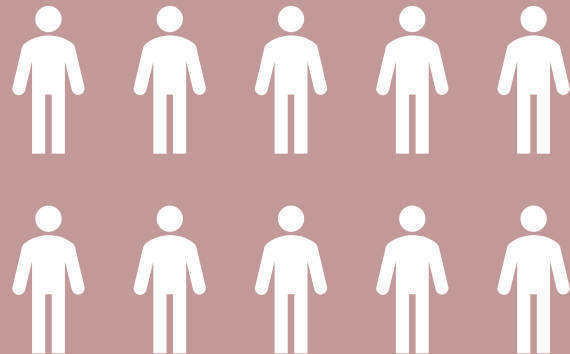
■ 10 000 активов, 30 000 EPS



Смотрит только наиболее критически опасные инциденты



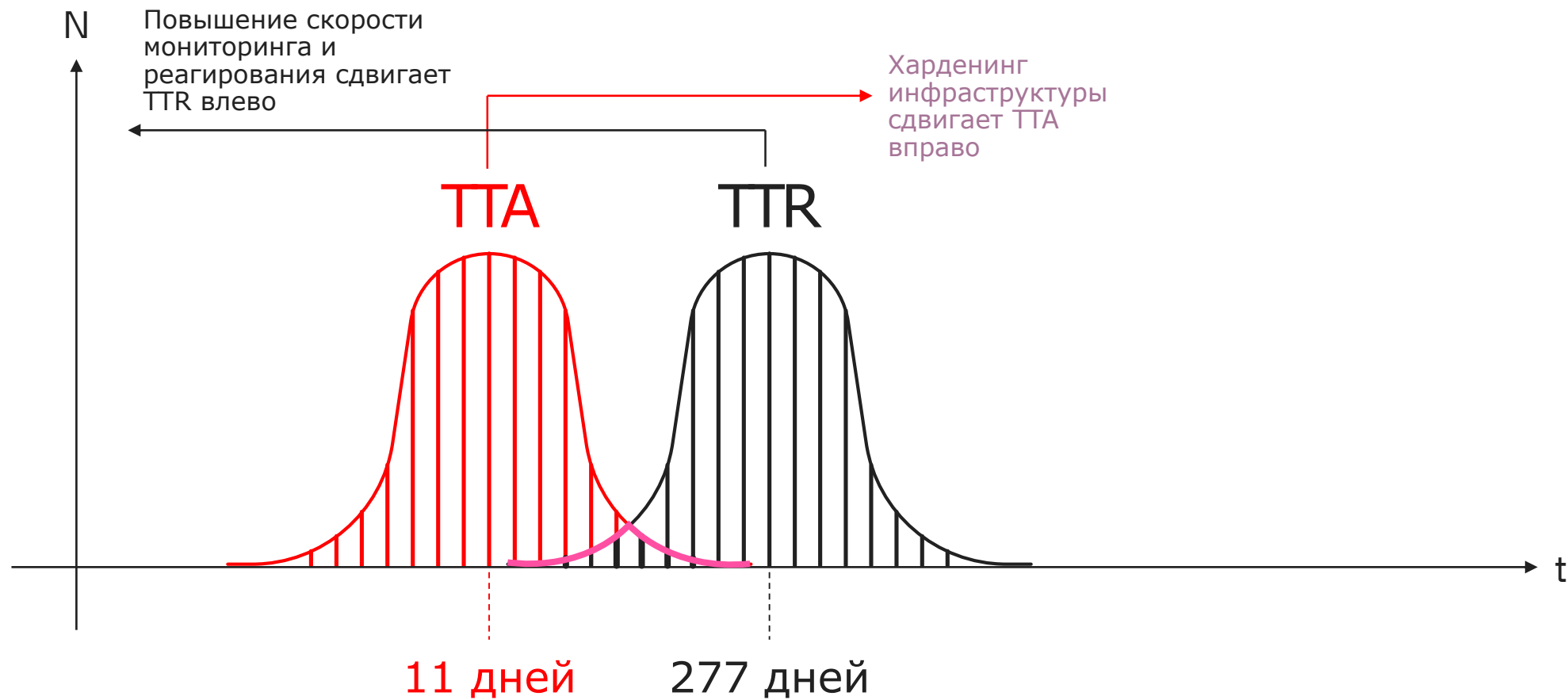
Смотрят все инциденты



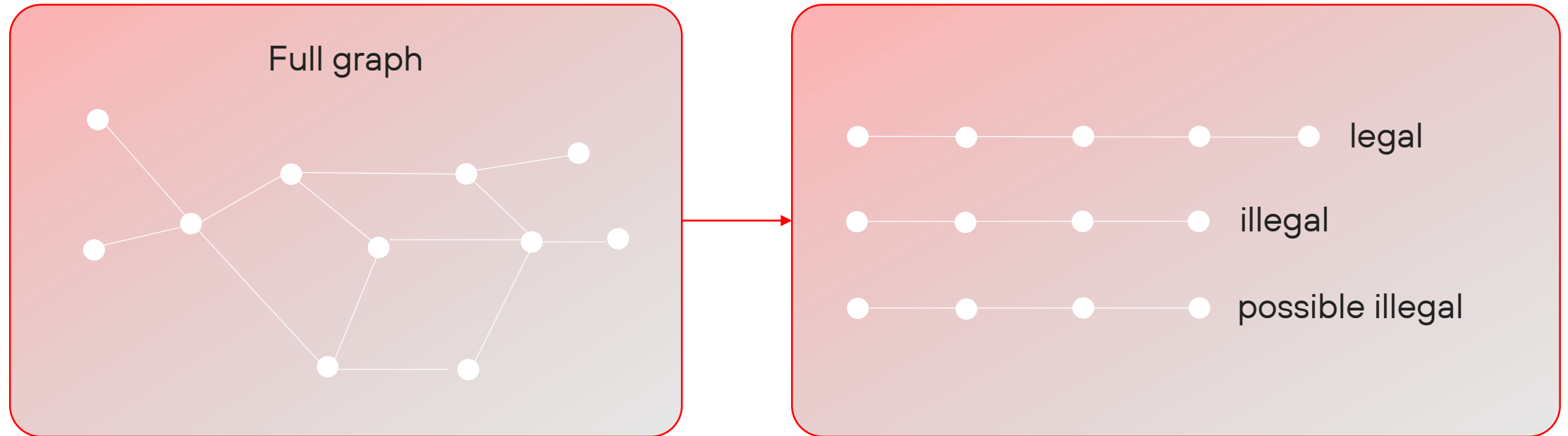
Смотрят все сработки СЗИ



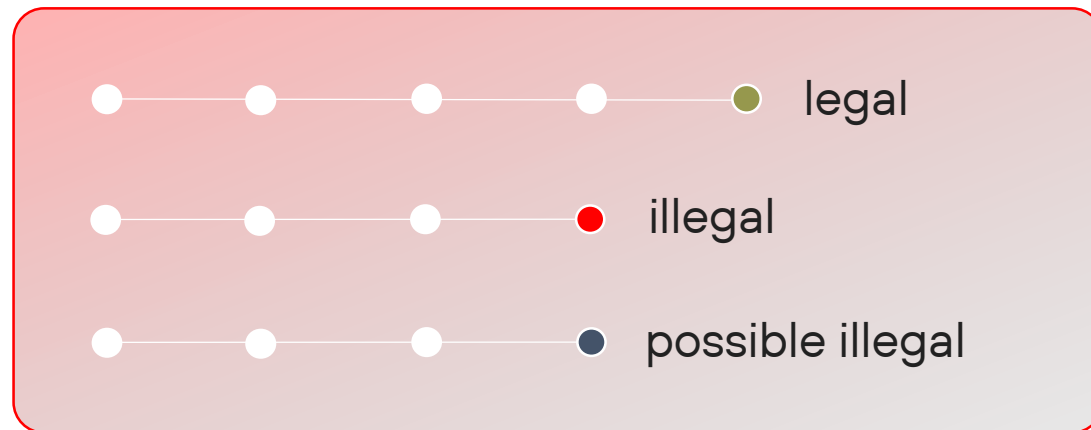
Атаки успешны, когда $TТА < TTR$



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 трафик в МСЭ между узлами «host – host»

Автопилот для результативной кибербезопасности



Обнаруживает
злоумышленника
и определяет, до каких
ресурсов ему удалось
добраться



Прогнозирует
сценарий развития
атаки с учетом
недопустимых
для компании событий



Останавливает
атаку до того,
как компании будет
нанесен непоправимый
ущерб

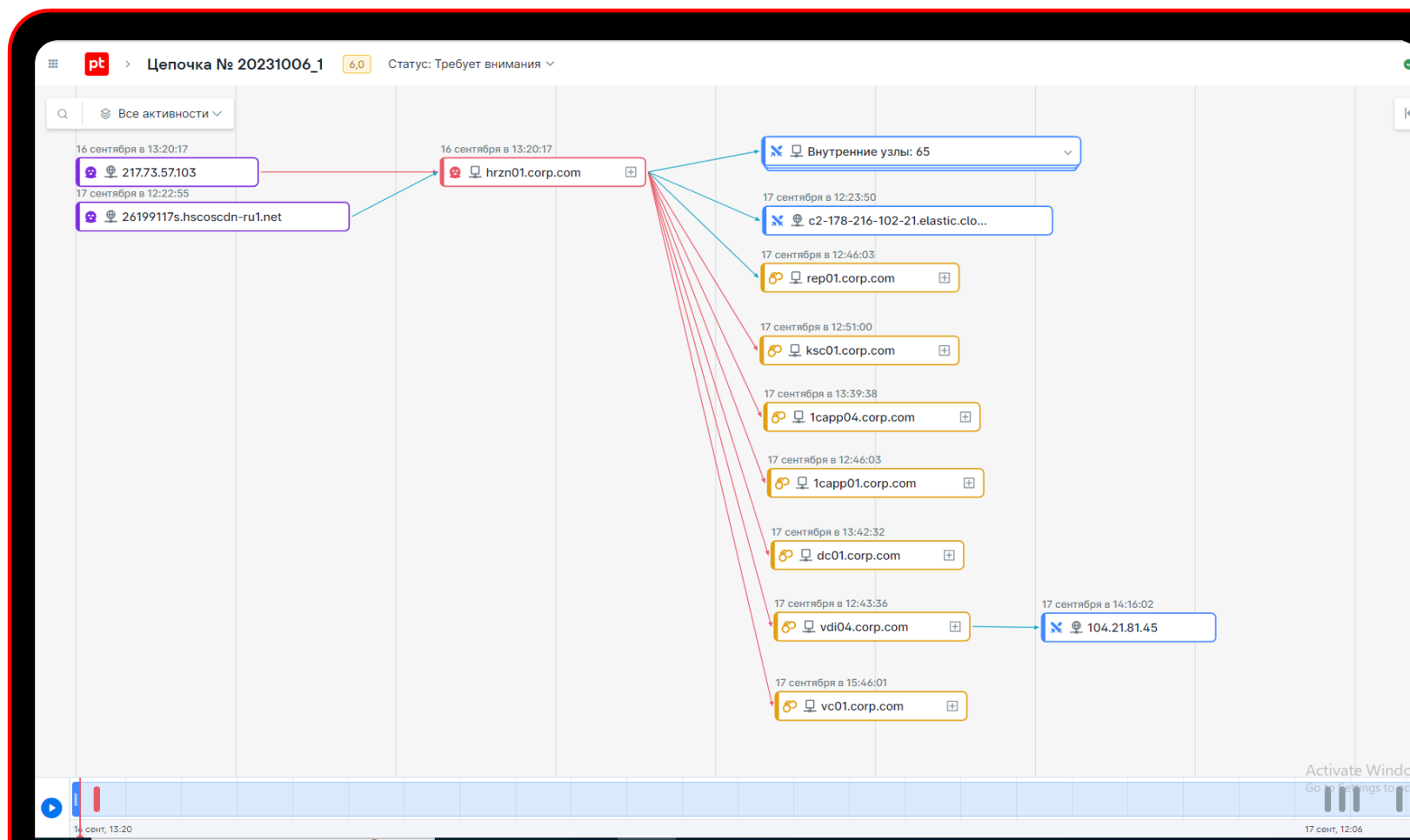
Выявление активности злоумышленников



Анализировать данные от сенсоров



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



Автоматизация расследования



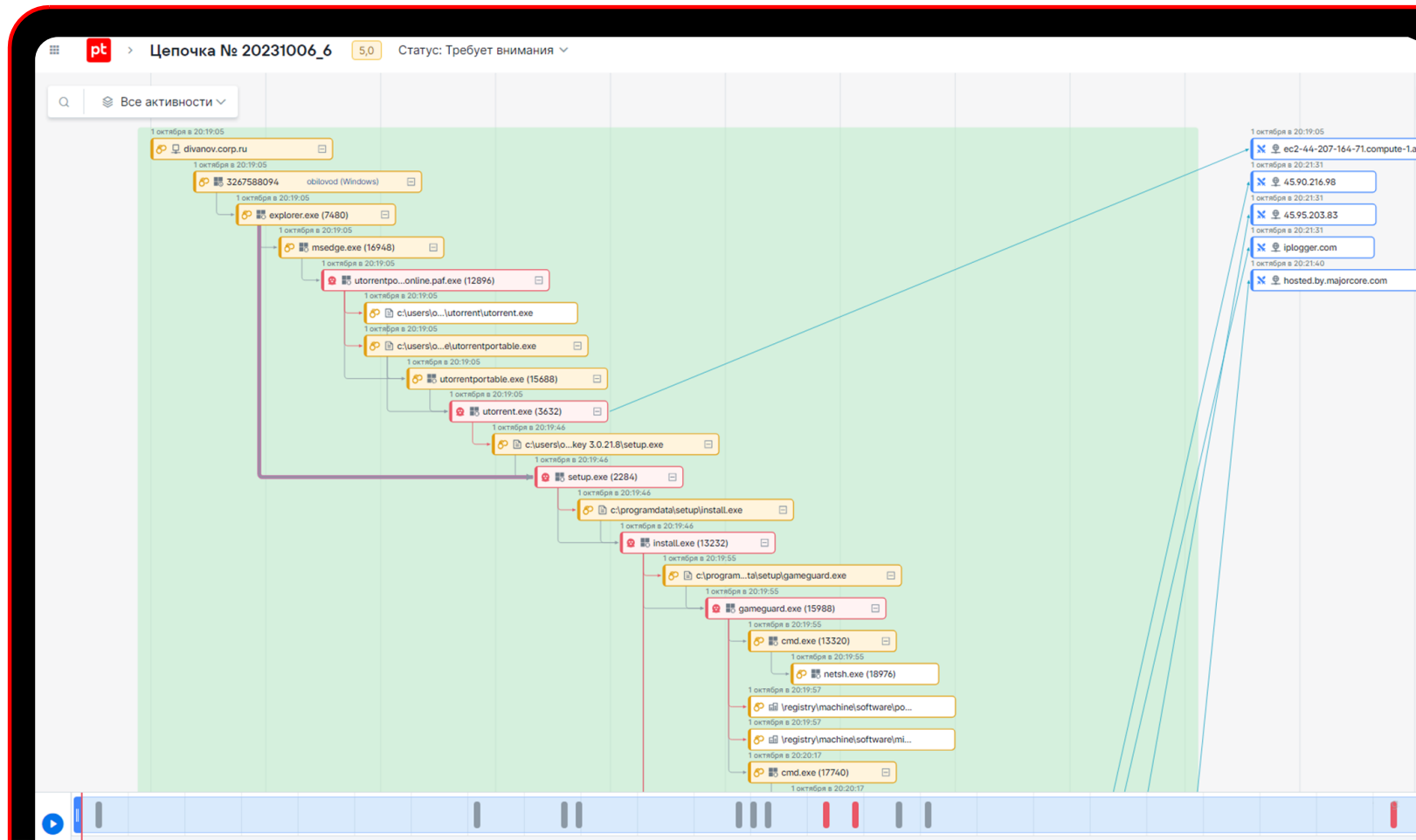
Проводить ретроспективный анализ продвижения злоумышленника



Определять способ проникновения в инфраструктуру, закрепления и продвижения



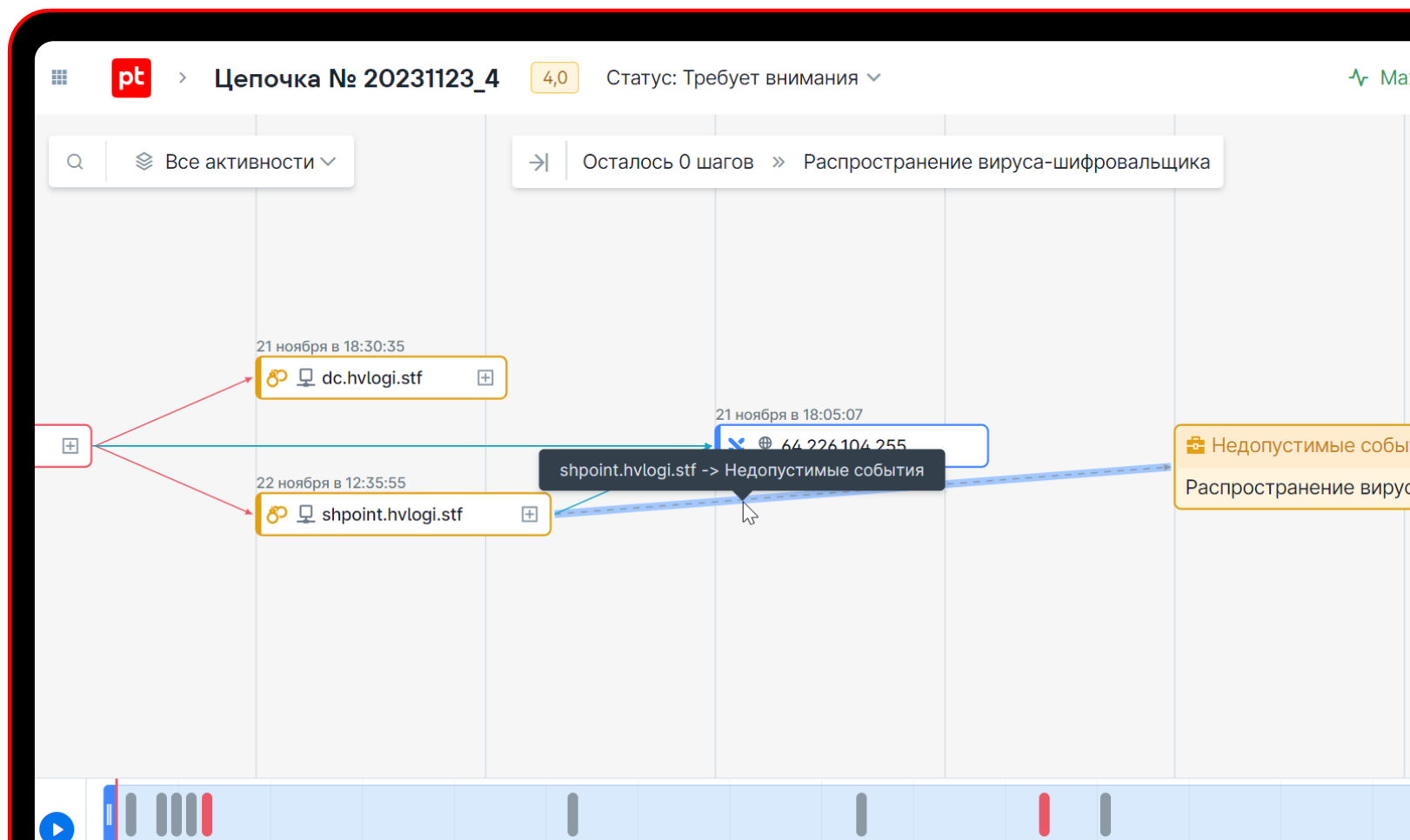
Восстанавливать хронологию атаки



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 «Требуется внимания» и привлекать эксперта только к действительно значимым активностям

Цепочка № 20230427_2	183,0	Архивная
Первое событие	27 апреля, 11:31	
Последнее событие	27 апреля, 11:42	
Количество событий	183	
Количество ресурсов	62	
Цепочка № 20230428_4	137,0	Архивная
Первое событие	28 апреля, 16:29	
Последнее событие	3 мая, 21:17	
Количество событий	142	
Количество ресурсов	132	
Цепочка № 20230429_15	122,0	Архивная
Первое событие	29 апреля, 18:00	
Последнее событие	2 мая, 08:26	
Количество событий	124	
Количество ресурсов	125	

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

The screenshot displays a security management interface. On the left, a diagram shows a response plan with nodes for external nodes, processes, and files. On the right, a list of actions is shown, including the successful deletion of a file.

Внешние узлы: 0 / 2

- 10.125.0.21
- 10.125.254.2

Процесс: 7 / 9

- bitsadmin.exe (616) Успешное реагирование
- certutil.exe (8604) Успешное реагирование
- cmd.exe (9296) Успешное реагирование
- explorer.exe (4324)
- installer.exe (5796) Успешное реагирование
- powershell.exe (1472) Успешное реагирование
- powershell.exe (7504) Успешное реагирование
- system (4)
- winword.exe (956) Успешное реагирование

Файл: 3 / 8

- c:\program...e\office16\winword.exe
- c:\users\user\documents\zarplata.doc Успешное реагирование
- c:\windows...ll\v1.0\powershell.exe
- c:\windows\syswow64\bitsadmin.exe

Действия История

- Удаление файла
Успешно: Сегодня, 15:16

Результаты киберучений – на практике



Классический подход

Сработок, требующих внимания

432

Время верификации и расследования

64 часа

Коэффициент обработанных сработок

83 %

Как меняется ситуация с автоматизацией

3

30 мин.

100 %

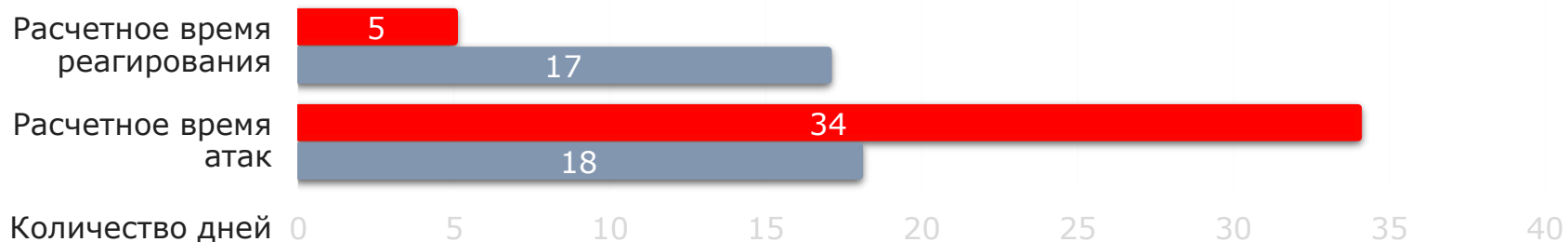
Время реагирования

<1 мин.

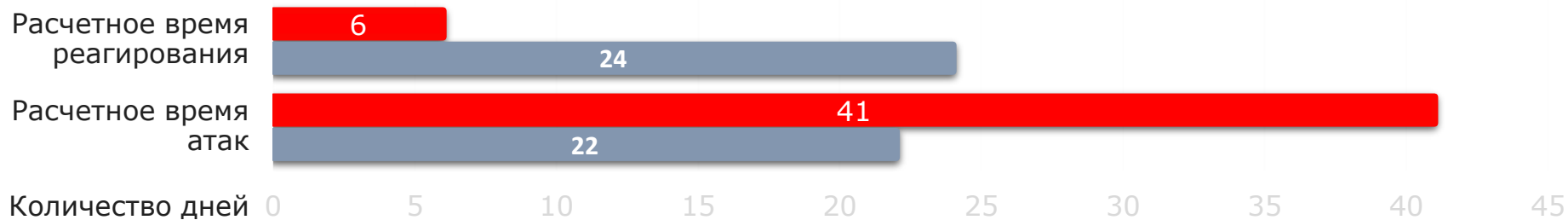
10 сек. Формирование сценария

30 сек. Выполнение

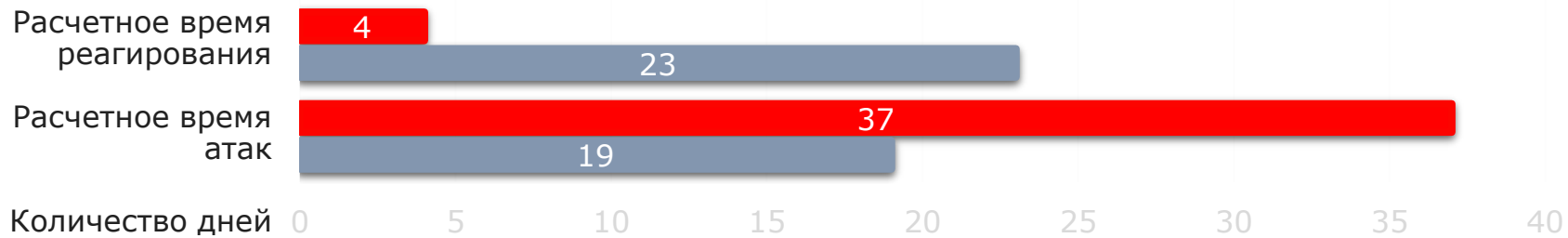
Результаты расчетных внедрений



Тип события:
недопустимое событие 1



Тип события:
недопустимое событие 2



Тип события:
недопустимое событие 3

После автоматизации Текущее

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

Спасибо
за внимание

