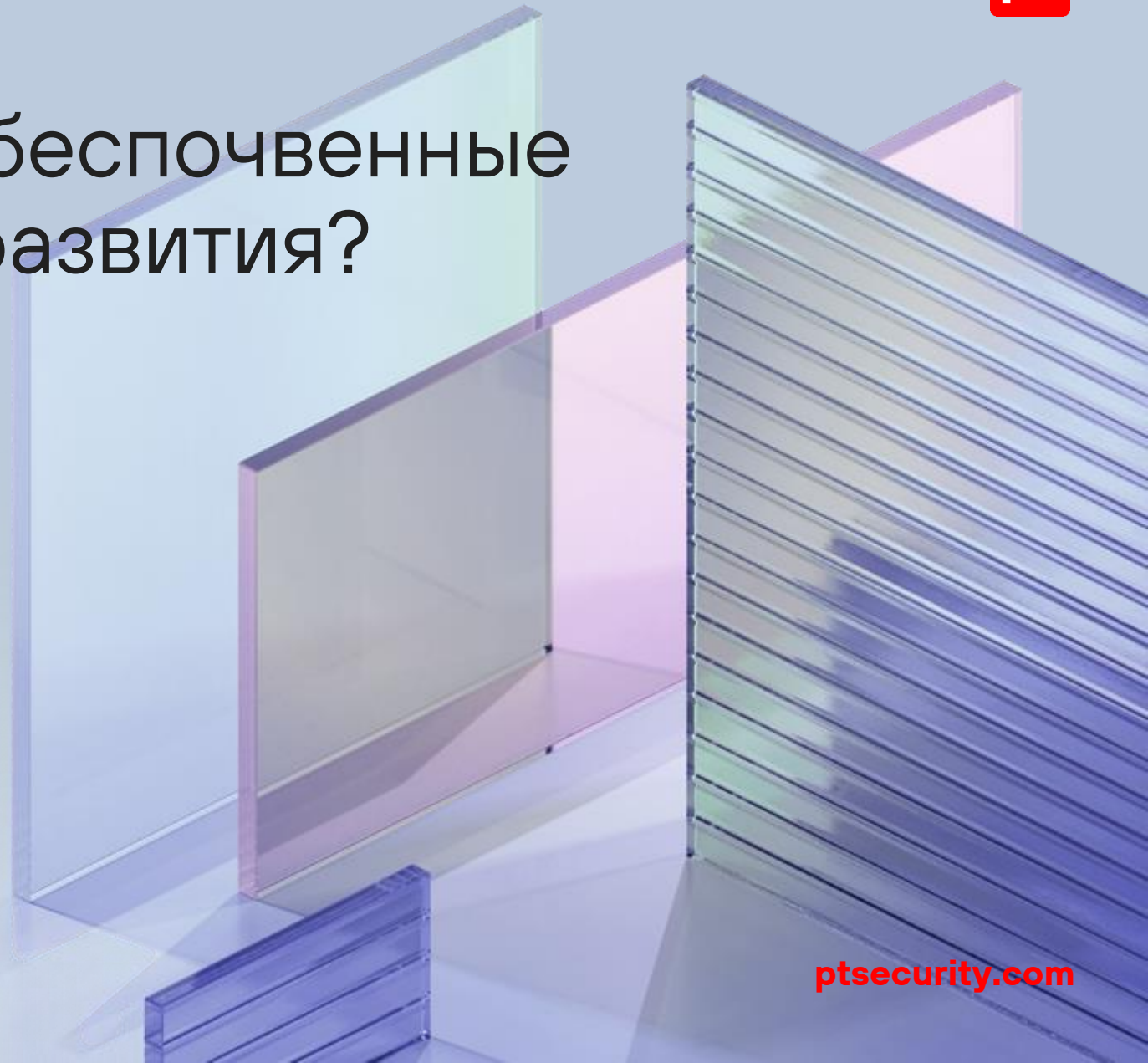
SOC на автопилоте - беспочвенные мечты или стратегия развития?

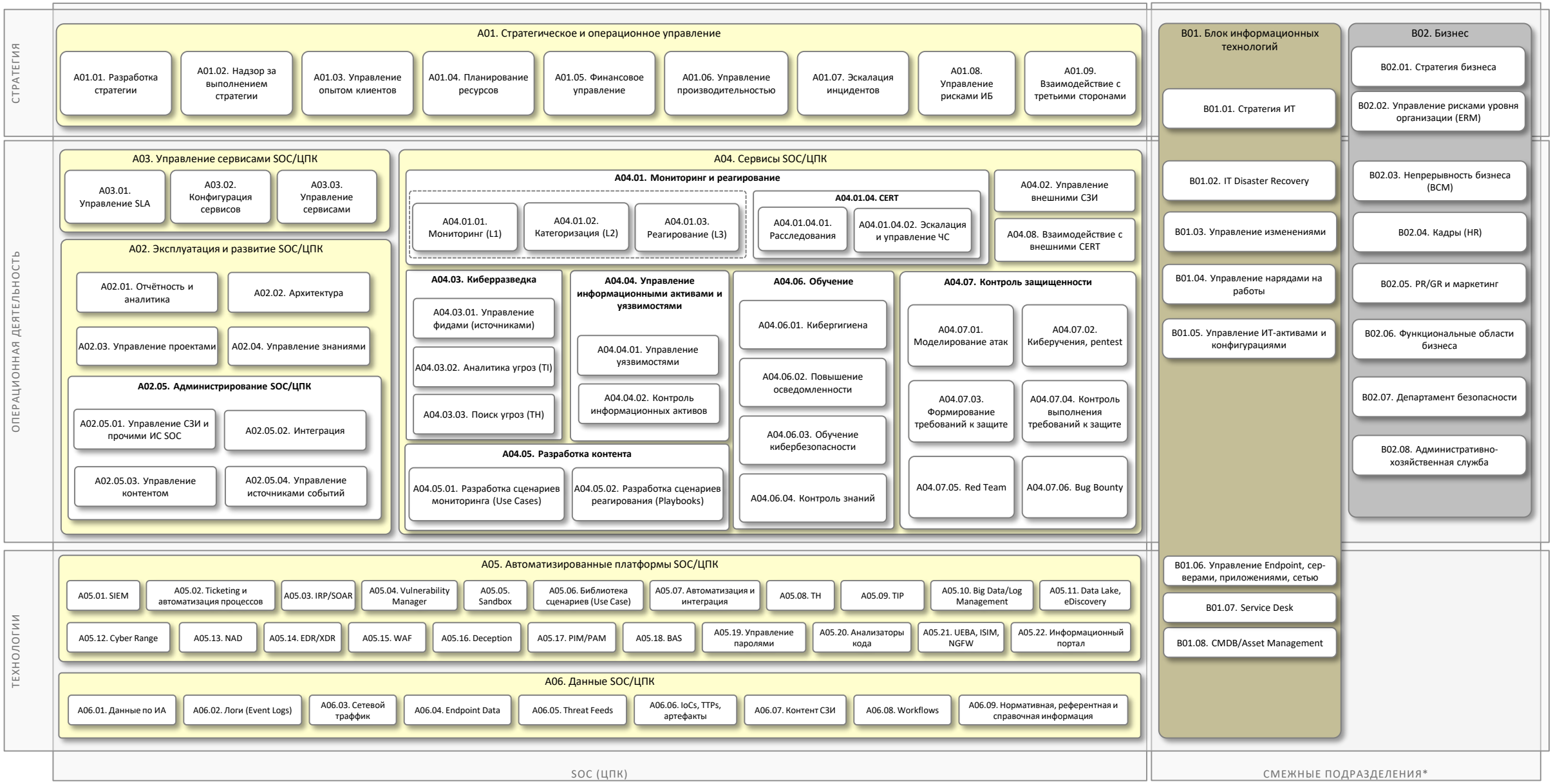
Михаил Кадер

АО «Позитив Текнолоджиз»

20.10.2023



Операционная модель SOC (спасибо Константину Смирнову)



Сходимость?

- Управление активами
- Управление уязвимостями
- Мониторинг и реагирование
- И многое другое ....

Недопустимые события

В каждой отрасли экономики есть события, которые недопустимы

— возникающие в результате действий злоумышленников события, приводящее к продолжительному нарушению, деградации или полной остановке процессов предприятия, отрасли, государства, и ставящее под угрозу достижение операционных и стратегических целей бизнеса или государственного управления

Воздействие кибератаки на организацию

- крупные финансовые потери
- публичные судебные разбирательства
- остановка производственных процессов
- потеря доли рынка
- срыв контрактных обязательств

Выполняет все свои функции	Выполняет свои функции частично	Не выполняет свои функции
		
допустимый ущерб	значительный ущерб	недопустимый ущерб

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.

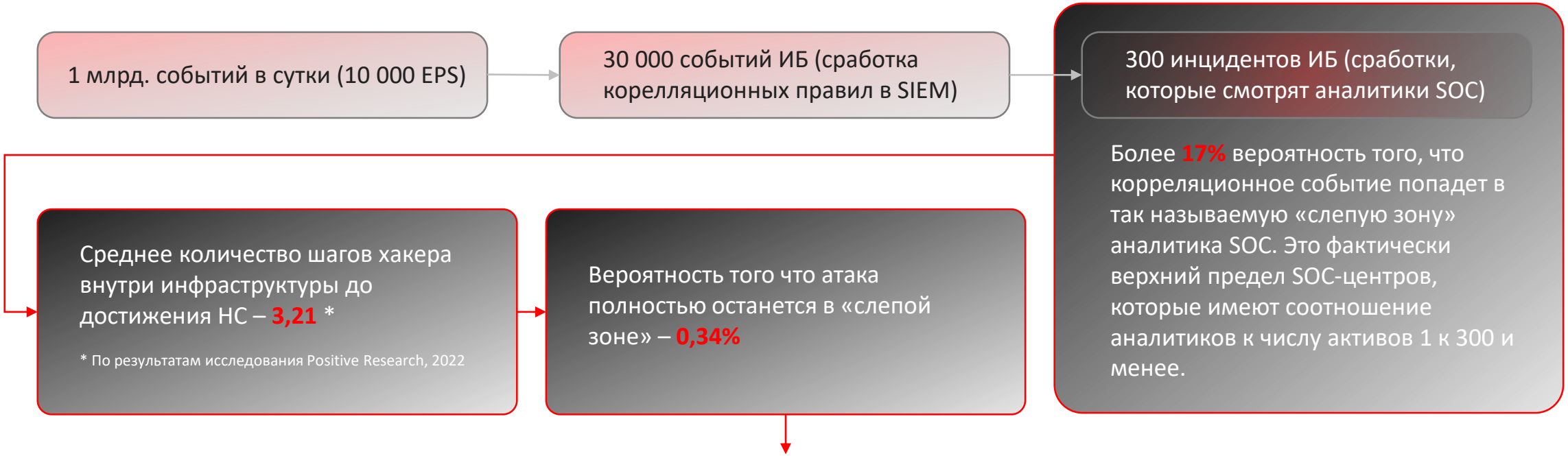
Проверка полноты и качества построения ЦПК и невозможности реализации недопустимых событий

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

Это панацея?

- Да?
- Скорее да?
- Скорее нет?
- Нет?
- Или?

Автоматизация – единственный способ полностью закрыть модель угроз



Даже при полностью выстроенной системе мониторинга и достаточной укомплектованности и компетентности штата аналитиков SOC остается достаточно высокий риски успешной реализации целевых атак на инфраструктуру компании.

Данный риск может быть закрыт только путем анализа и расследования всех сработок ИБ решениями автоматизации (класс AHDR)

Решения по автоматизации [ИБ]

Решение по автоматизации [ИБ] – это совокупность программных и аппаратных решений вместе с набором пред-эксплуатационных сервисов, позволяющих заместить один из **процессов** [обеспечения ИБ] в организации полностью или частично устранив из него человека.

Процесс [ИБ] – определяется набором измеримых показателей его целевой функциональности. По-другому такой набор обозначим как «**результат**»

Классическое решение – определяется совокупностью функций

Примеры функций:
- Возможность формирования маршрута заявки в Helpdesk;
- Автоматический reboot серверов после сбоя;
- Написание правил корреляции для детектирования возможной нелегитимной активности

Классы решений ИБ: SIEM, VM, NTA, SB, …

Решение по автоматизации – определяется совокупностью результатов

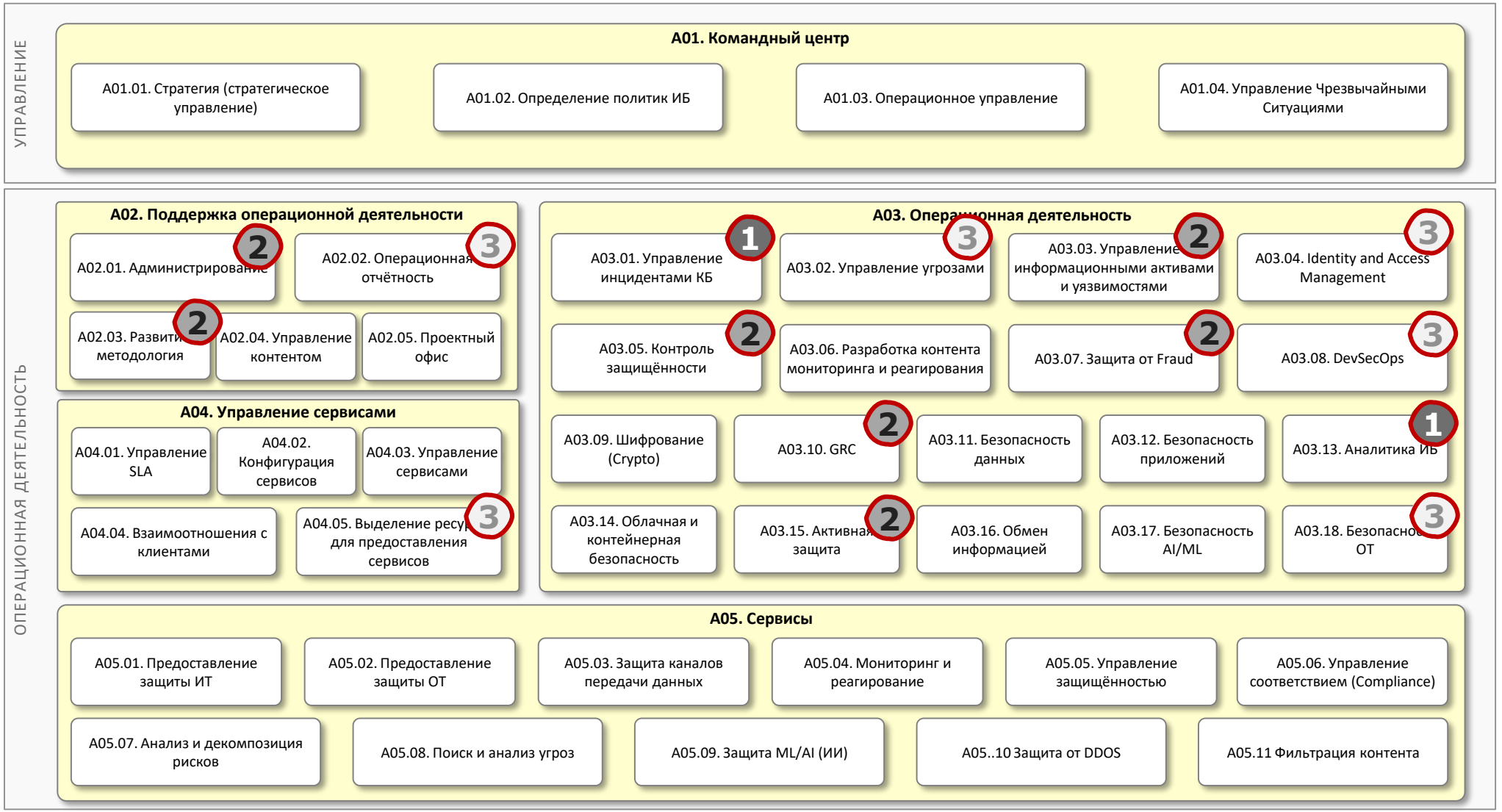
Примеры результатов:
- Заявка в helpdesk отрабатывается в течении 5 минут с ее регистрации
- Показатель RTO по восстановлению работоспособности сети не превышает 10 минут
- Движение хакера в инфраструктуре будет гарантированно обнаружено при совершении им не более 3 шагов по продвижению к реализации риска

Классы решений автоматизации ИБ: ???

Дерево результатов по кибербезопасности

Немного практики

Применение автоматизации для уменьшения участия человека (1/2)



Примечание:
(1) – большое количество функций может быть автоматизировано тем или иным образом, большая ценность результата. (2) некоторые функции могут быть автоматизированы, заметная ценность результата. (3) только отдельные функции могут быть автоматизированы, ценность заметна только на отдельных функциях (лучше декомпозировать дальше), существенная сложность в реализации снижает ценность.

Применение автоматизации для уменьшения участия человека (2/3)

A03. Операционная деятельность

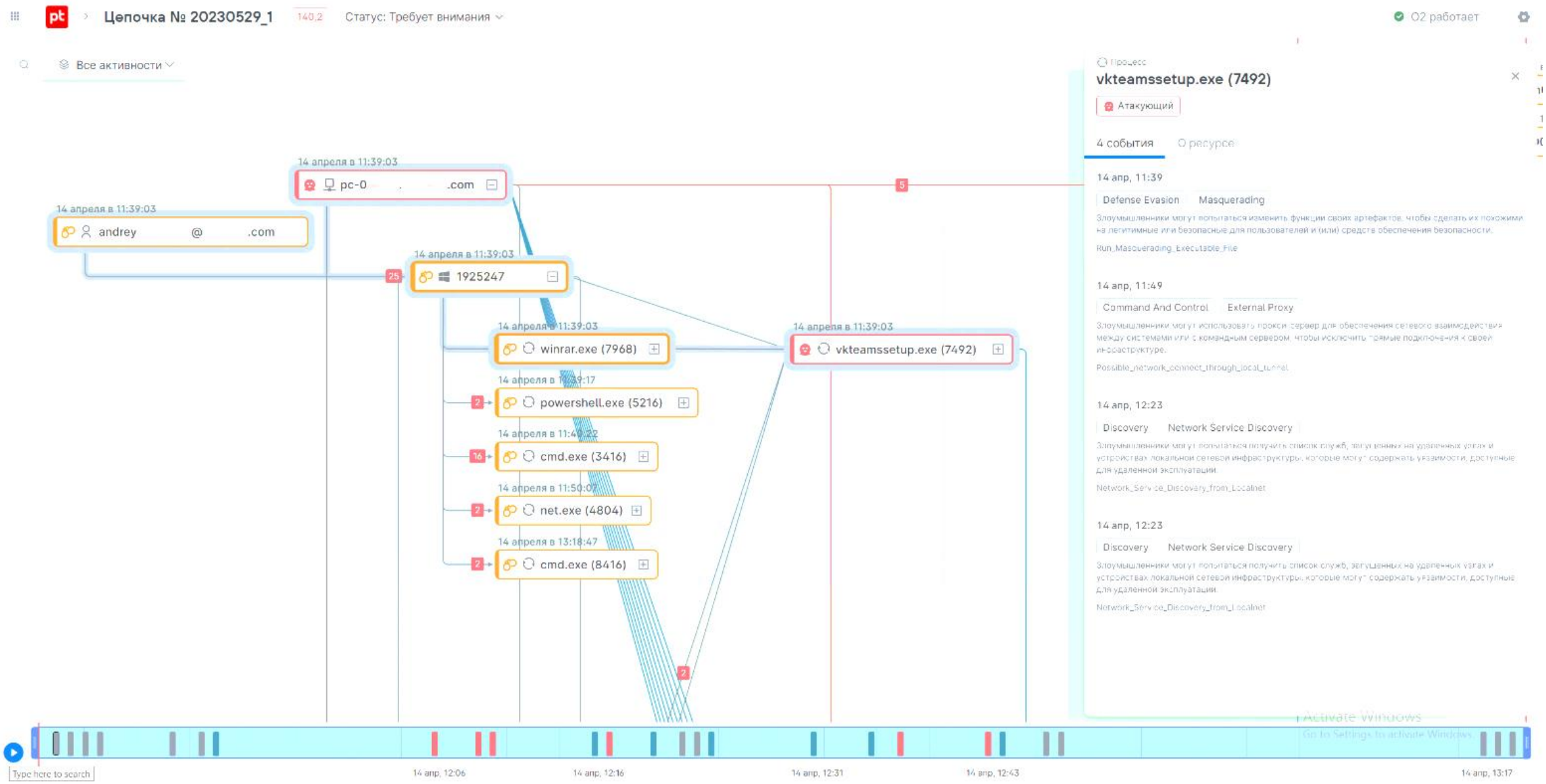
Функция/сервис	Насколько	Какая автоматизация
A03.01. Управление инцидентами ИБ	1	• Определение False Positives (NN) • Категоризация/определение приоритетов ИИБ (NN) • Обогащение ИИБ (AU, AI?) • Реагирование на простые инциденты (AI) • Статус - как идёт реагирование на инциденты (AU) • Маршрутизация инцидентов (AI) • Логика процесса (AU) • Forensics, расследования – обобщение результатов, поиск совпадений с другими кейсами (AI) • Lessons learned – обогащение базы знаний, поиск совпадений с другими кейсами (AI)
A03.02. Управление данными об угрозах	3	• Анализ репутации источников данных об угрозах (NN) • Аналитика угроз – оценка релевантности, выдача рекомендаций (AI) • Поиск угроз (ретро), outliers/аномалии (сеть, пользовательское поведение), (AI, NN?)

A03. Операционная деятельность (contd.)

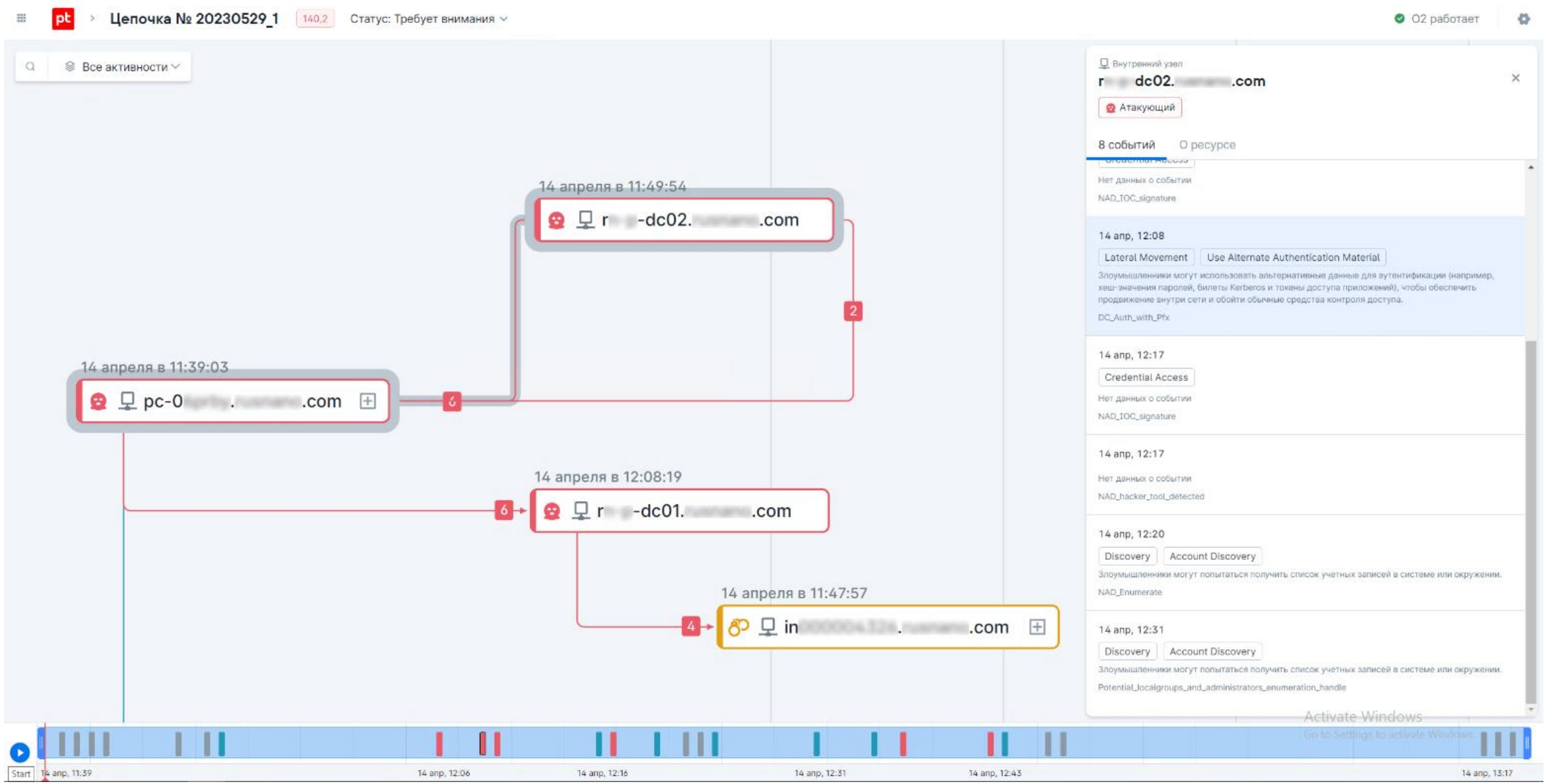
Функция/сервис	Насколько	Какая автоматизация
A03.03. Управление информационными активами и уязвимостями	2	• Категоризация/определение приоритетов уязвимостей (NN) • Выдача рекомендаций по уязвимостям (в том числе – подбор оптимальных контролей) (AI) • Отчёты и статус/контроль - как идёт закрытие уязвимостей (AU) • Логика процесса (AU) • Дедупликация, обогащение, управление жизненным циклом активов (AI?)
A03.04. Identity and Access Management	3	• Постоянная аутентификация пользователей через анализ поведения (AI/NN?) • Анализ ролей и авторизации на предмет соответствия политикам (AI?) • Логика процесса (AU)
A03.05. Контроль защищённости		• Моделирование атак на цифровом двойнике ИТ (AI, AU) • Генерация решений (наборов контролей) из профиля угроз/атак и ландшафта уязвимостей (AI, AU) • Непрерывный контроль выполнения требований к защите (AI, NN)

Примечание:
Графа «Насколько». (1) – большое количество функций может быть автоматизировано тем или иным образом, большая ценность результата. (2) некоторые функции могут быть автоматизированы, заметная ценность результата. (3) только отдельные функции могут быть автоматизированы, ценность заметна только на отдельных функциях (лучше декомпозировать дальше), существенная сложность в реализации снижает ценность.
Графа «Какая автоматизация». NN – нейросеть, решает одну специализированную задачу (например, False Positives). AI – генеративная модель широкого профиля, AU – обычная алгоритмическая автоматизация (если-то, скрипты)

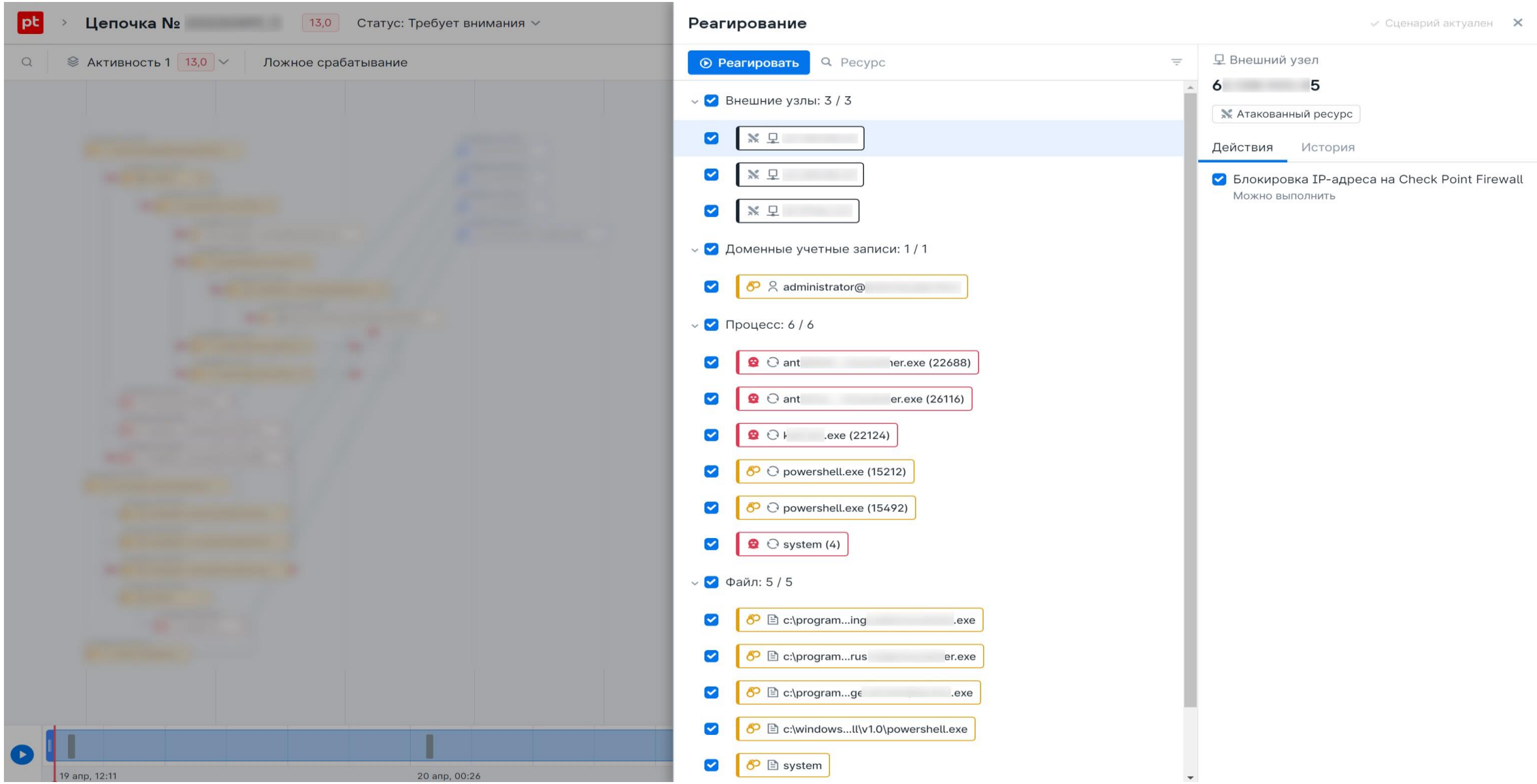
Случай из жизни (1/3)



Случай из жизни (2/3)



Случай из жизни (3/3)



- Автоматизация – наше все ☺
- Автоматизировать можно не все
- Недопустимые события - путь к повышению эффективности автоматизации

Спасибо
за внимание

ptsecurity.com