PT
Информационная
безопасность

Another brick in the SOC

Как выстроить процесс взаимодействия TI с EDR в объёмах коммерческого SOC

Константин Васильев
Руководитель направления мониторинга и реагирования RT Protect SOC

АО «РТ-Информационная безопасность»

более 100

специалистов из ведущих технических ВУЗов

Собственная экосистема продуктов ИБ

Единый центр компетенций по ИБ в ГК «Ростех»

Константин Васильев

Руководитель направления мониторинга и реагирования RT Protect SOC

@Constantine63

- Владелец продукта RT Protect TI
- Опыт Malware Analysis, DFIR 6+ лет

РТ
Информационная безопасность

Как мы видим разведку угроз?

- Определение мотивов, целей, тактик и техник атакующих
- Актуализация экспертизы
- Пополнение базы знаний об актуальных угрозах

PT
Информационная безопасность

Как применяем разведку угроз?

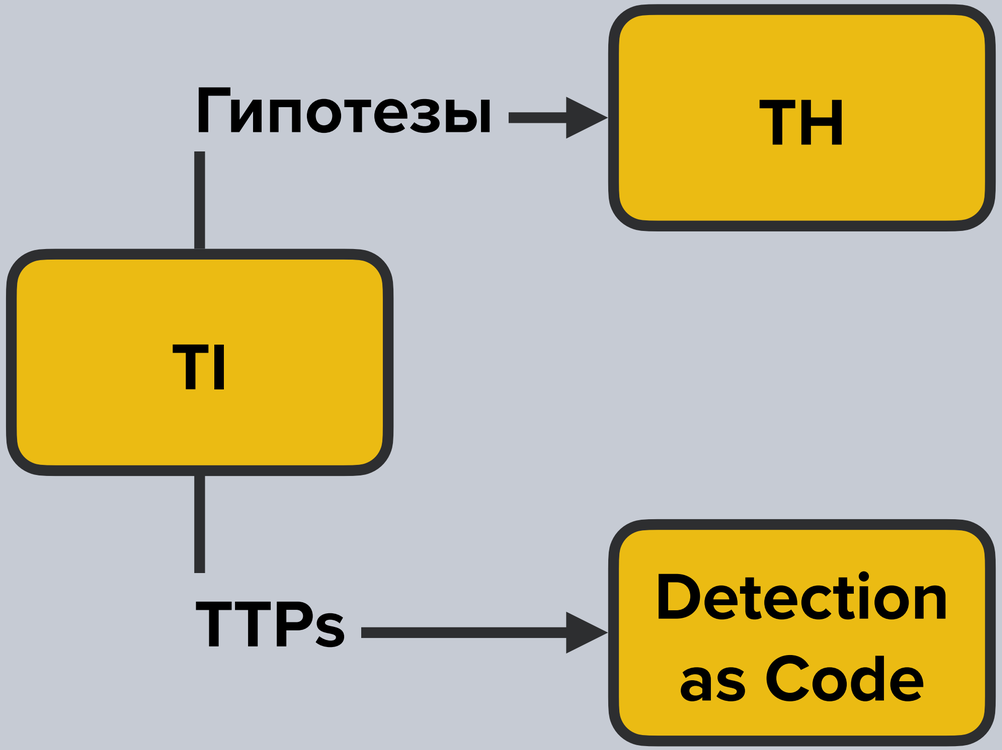
- Анализ угроз, зафиксированных в инфраструктуре Заказчиков
- Обогащение при расследовании инцидентов
- Основа реагирования – **EDR**
- Приоритет: **проактивная защита**

PT
Информационная безопасность

Как применяем разведку угроз?

- Формирование гипотез в рамках Threat Hunting
- Источник данных при разработке правил корреляции

  → **Detection as Code**



PT
Информационная безопасность

Как оценивать развитие TI?

PT Информационная безопасность

Уровни TI

Уровень	Ключевое слово	Период актуальности	В основе анализа	Потребители
04. Стратегический	Кто? Почему?	Долгосрочный (несколько лет)	Широкомасштабные кампании, группы, атаки со множеством жертв	CISO, CIO, CTO, GRC, высокоуровневая аналитика
03. Тактический	Как? Где?	Длительный (один год или чуть больше)	Семейства вредоносных программ, APT-группировки, анализ действий личностей	Threat Hunting, Incident Response, SOC аналитики
02. Оперативный	Что?	Средний (несколько месяцев)	События безопасности, экземпляры ВПО, инфраструктура злоумышленников, фишинговые письма	SIEM, IDS/IPS, EDR и т.д.
01. Технический	Что конкретно?	Короткий (несколько недель)	Отдельные индикаторы компрометации и индикаторы атак, характеризующие конкретную вредоносную активность (ветки реестра, пути, имена и хэши файлов)	

Развитие аналитики

PT
Информационная безопасность

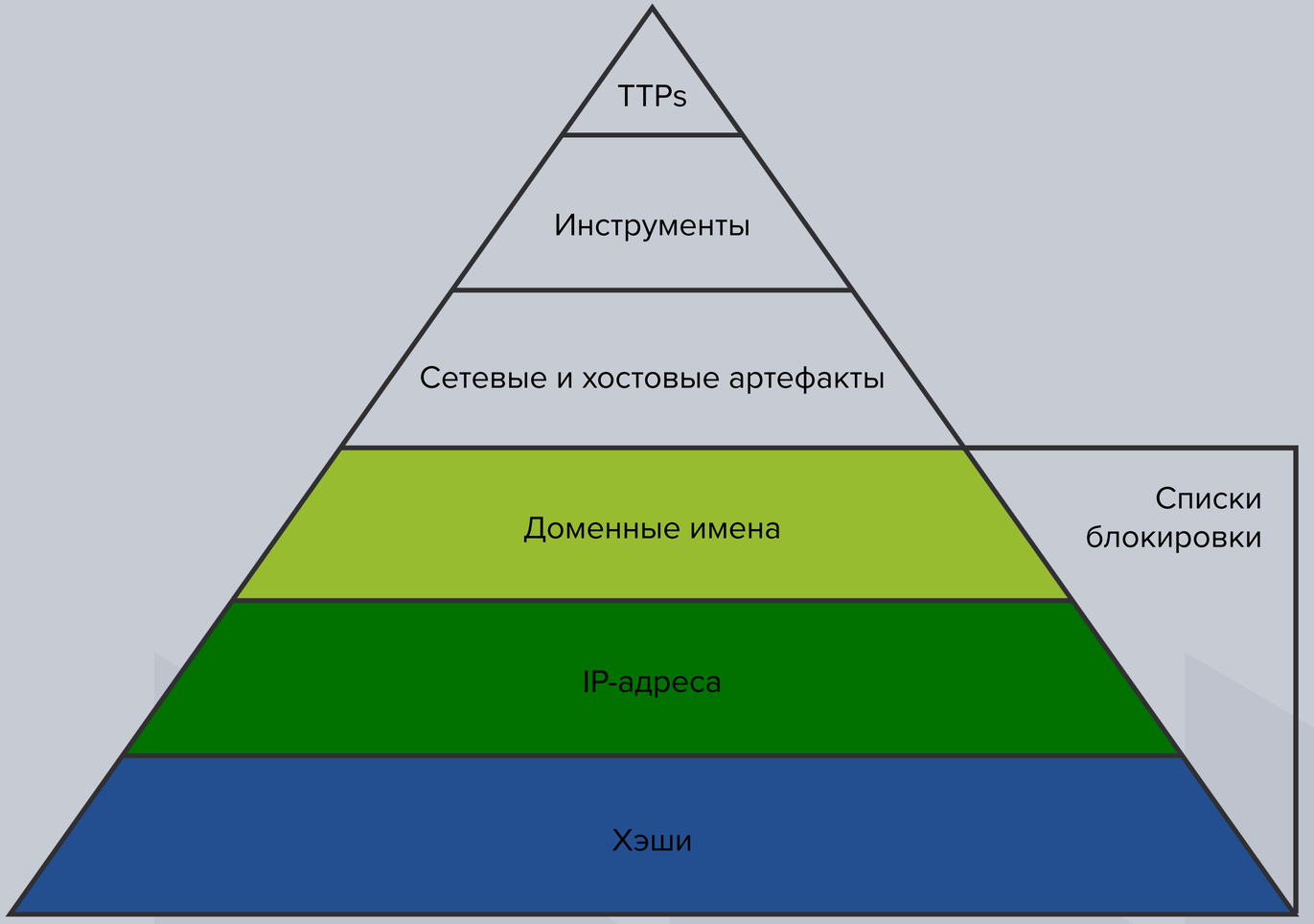
- С чего начать?
- Как выстроить процессы?

Стратегический

Тактический

Оперативный

Технический



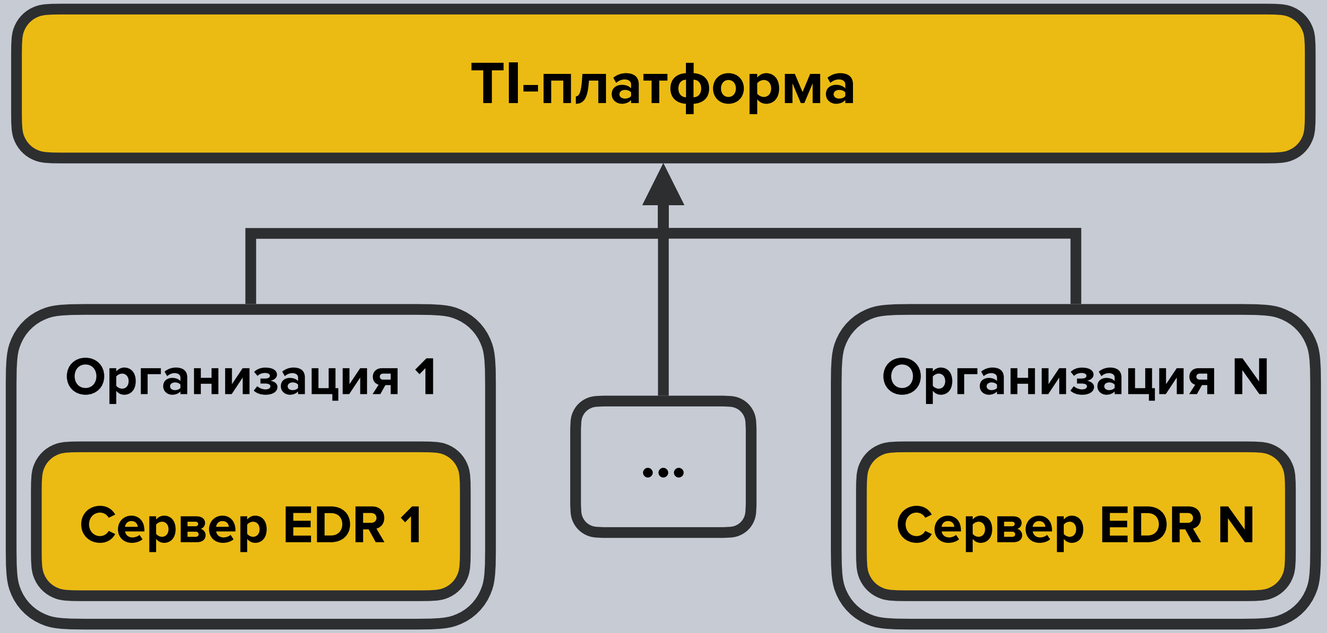
Развитие аналитики

- Выделим этапы развития **TI-платформы** в интеграции с **EDR**
- Построим **таймлайн** развития
- Оценим **результаты**

PT
Информационная безопасность

Вокруг чего выстраивать процессы TI?

- TI-платформа
- Основные функции:
  - Сбор и анализ данных из фидов (TI Feeds)
  - Интеграции со сторонними сервисами (VT, решения класса Sandbox и т.д.)
  - Применение IOC и IOA в EDR для активной блокировки угроз
  - Обогащение данных событий, инцидентов
  - Аналитика угроз



Фундамент – сервер аналитики артефактов

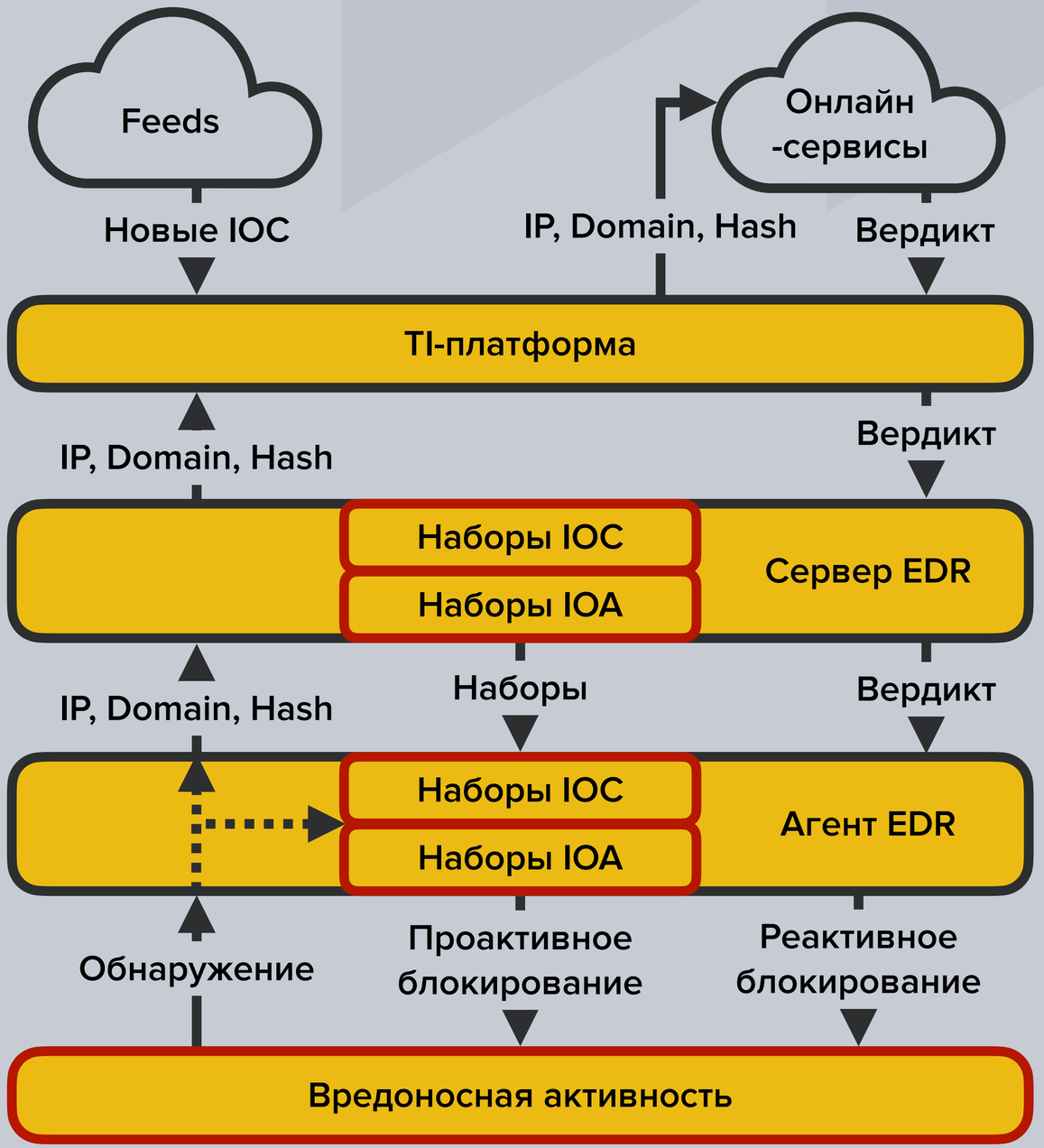
PT
Информационная безопасность

- WEB-Интерфейс
- Проверка артефактов: Hash, Domain, IP, URL
- Интеграция с EDR для проверки артефактов
- Фиды с черными и белыми списками
- Проверка IOC по бесплатным сервисам

Интеграция с EDR

- **Проактивное** блокирование вредоносной активности по спискам IOC и IOA
- Обогащение данных об артефактах в потоковом режиме:

  При получении вердикта с TI-платформы угроза блокируется в реактивном режиме, постфактум.



PT
Информационная безопасность

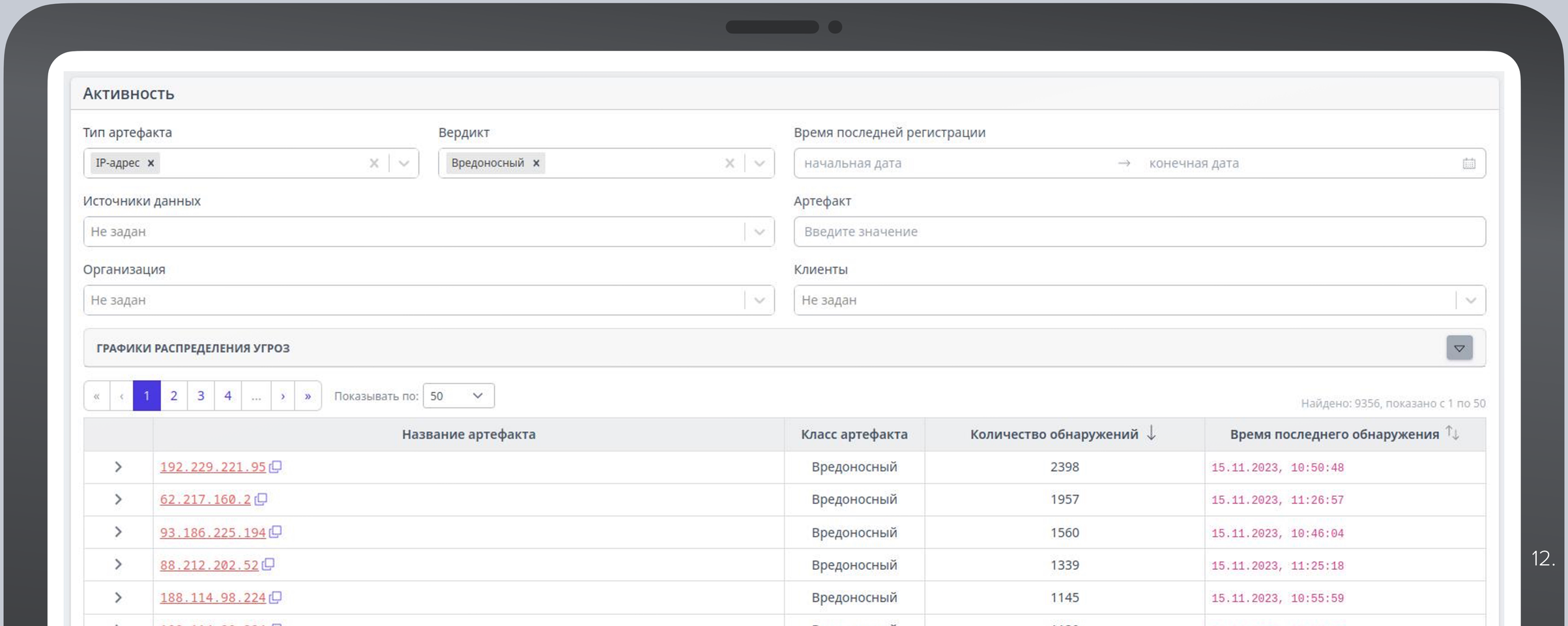
Brick 1

PT
Информационная безопасность

Brick 1

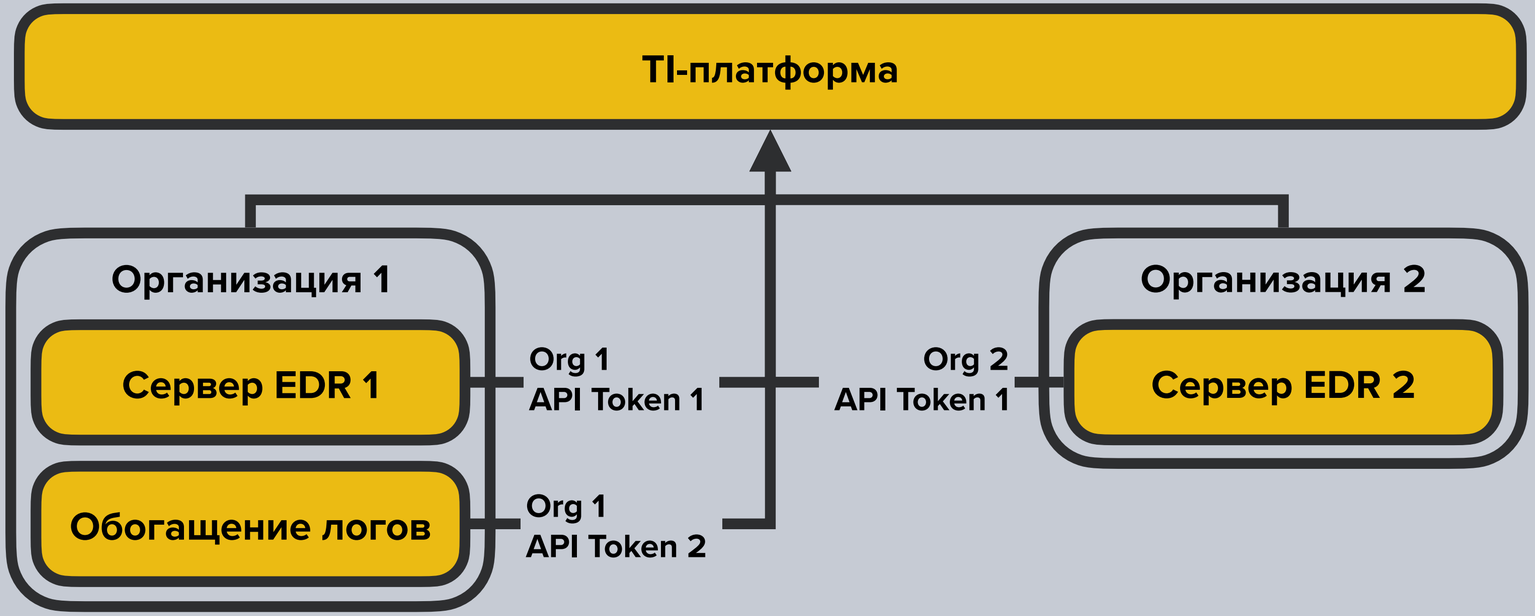
PT Информационная безопасность

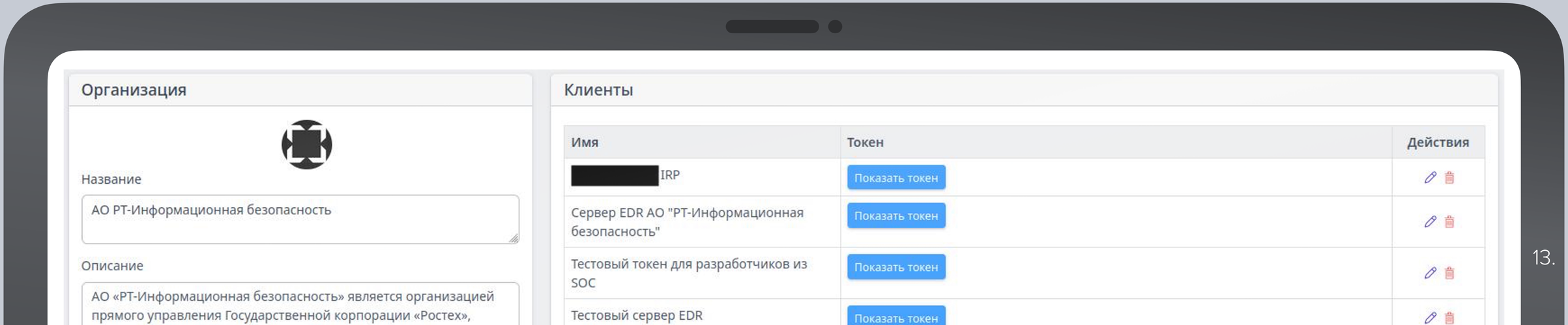
Страница с обнаружениями



Brick 1

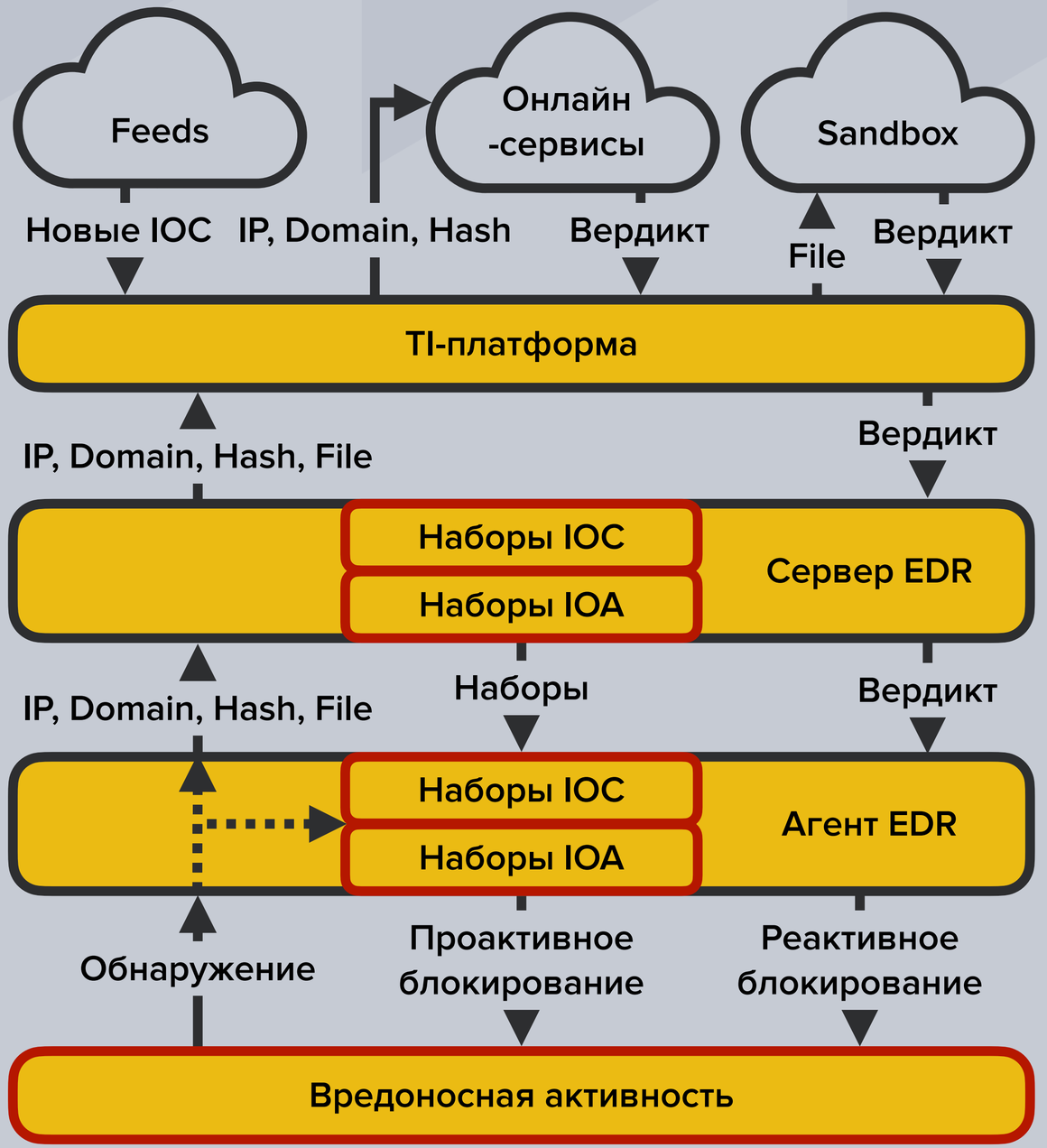
Менеджмент подключенных клиентов (интеграций)





Brick 1

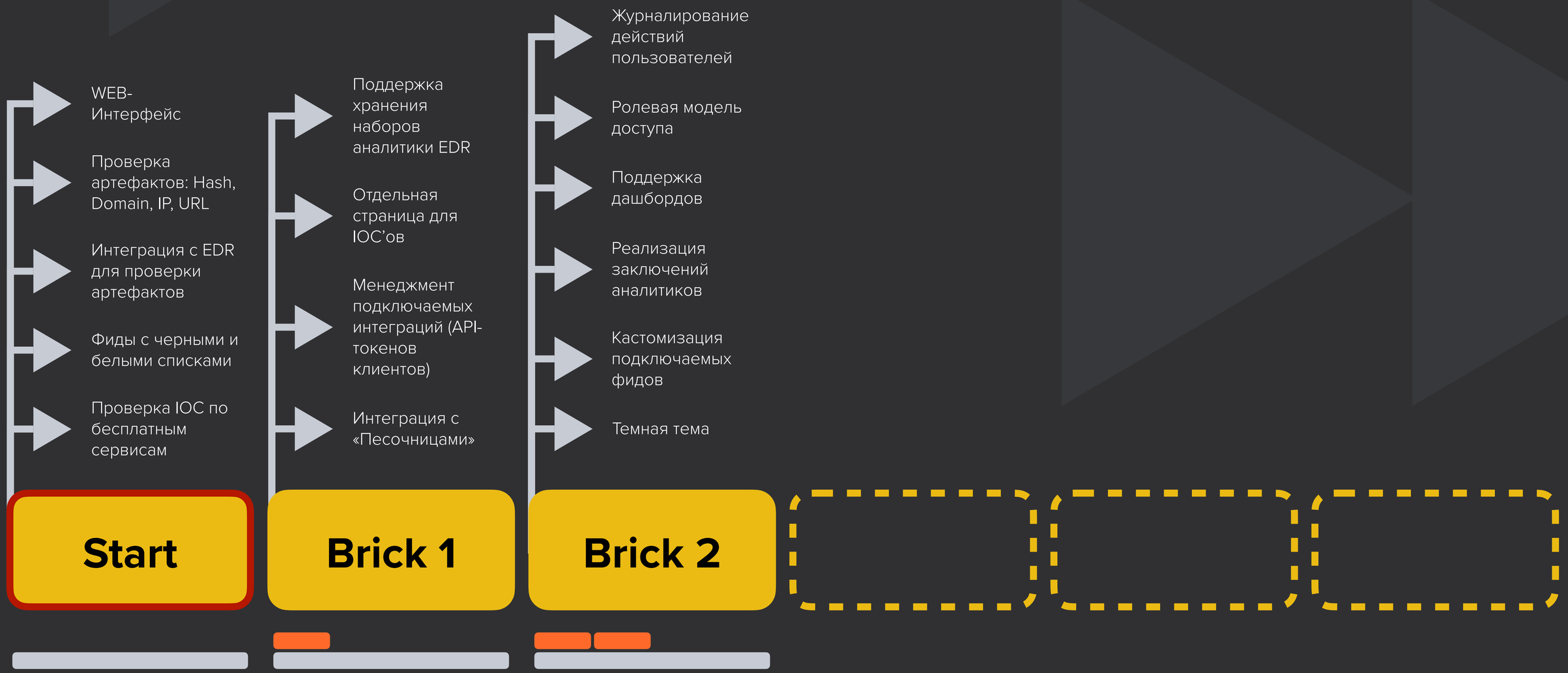
- Отправка файлов с EDR на проверку
- Интеграция с “песочницами”



PT
Информационная безопасность

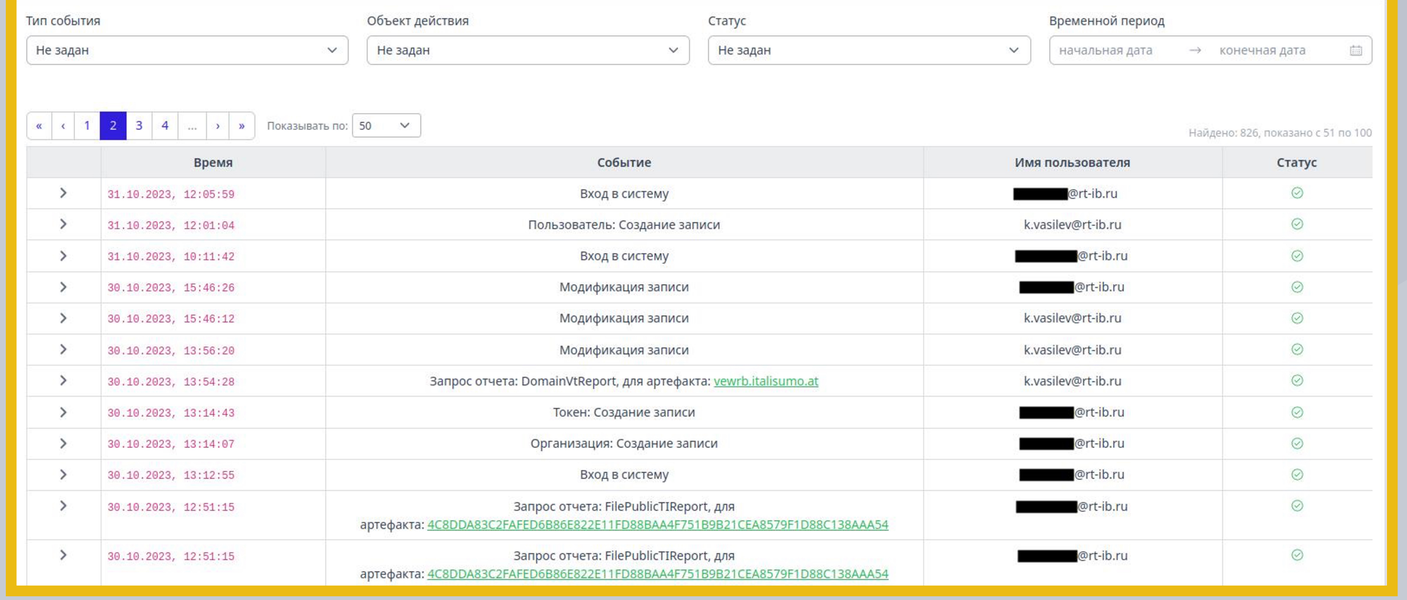
Brick 2

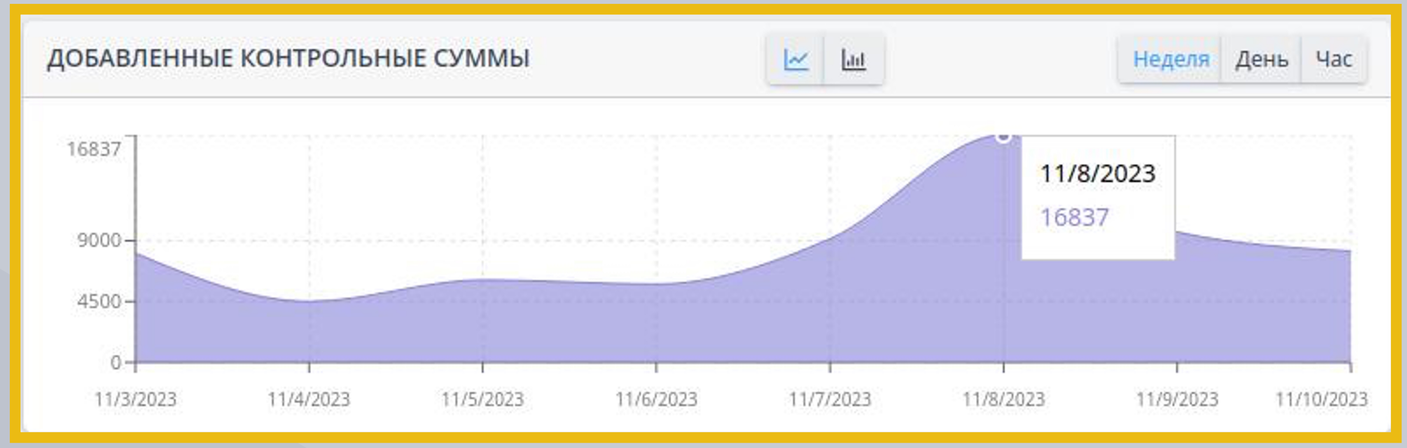
PT
Информационная безопасность

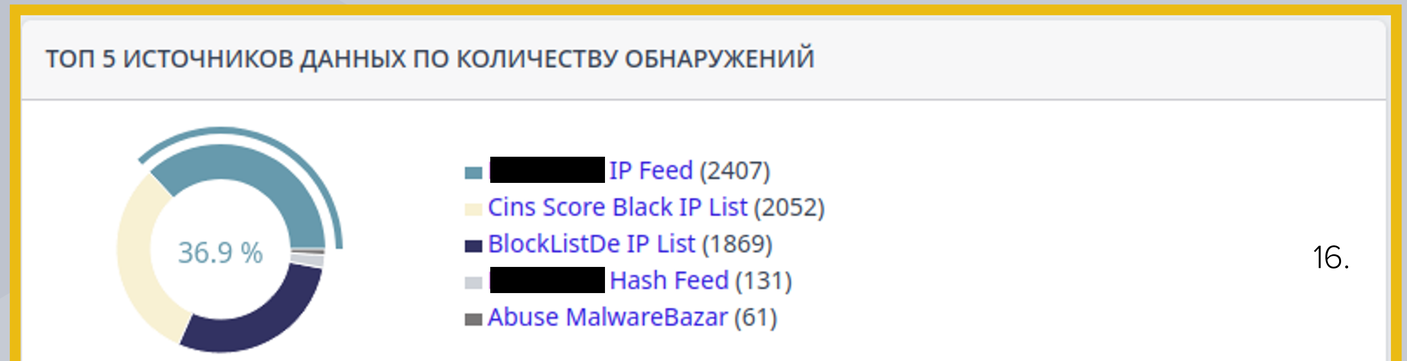


Brick 2

- Журналирование действий пользователей
- Ролевая модель доступа
- Реализация дашбордов



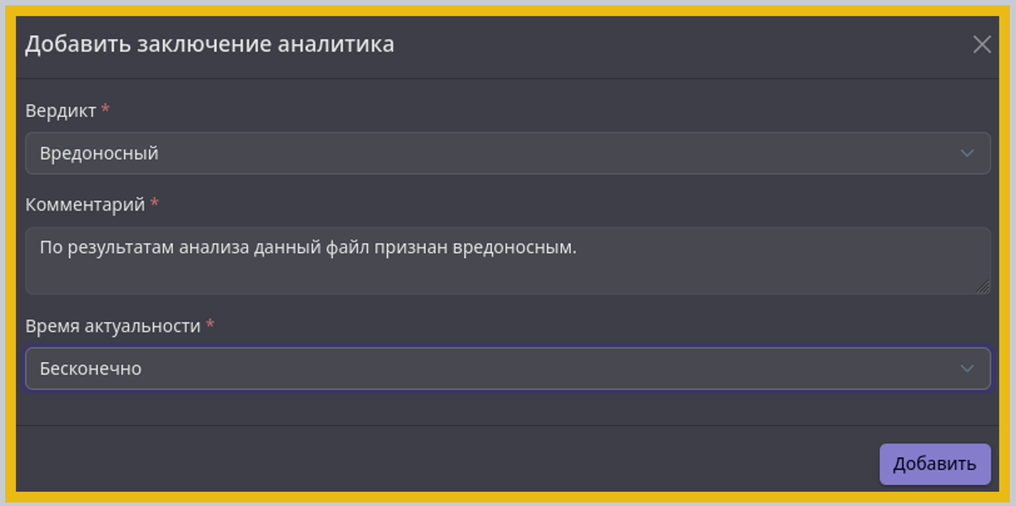


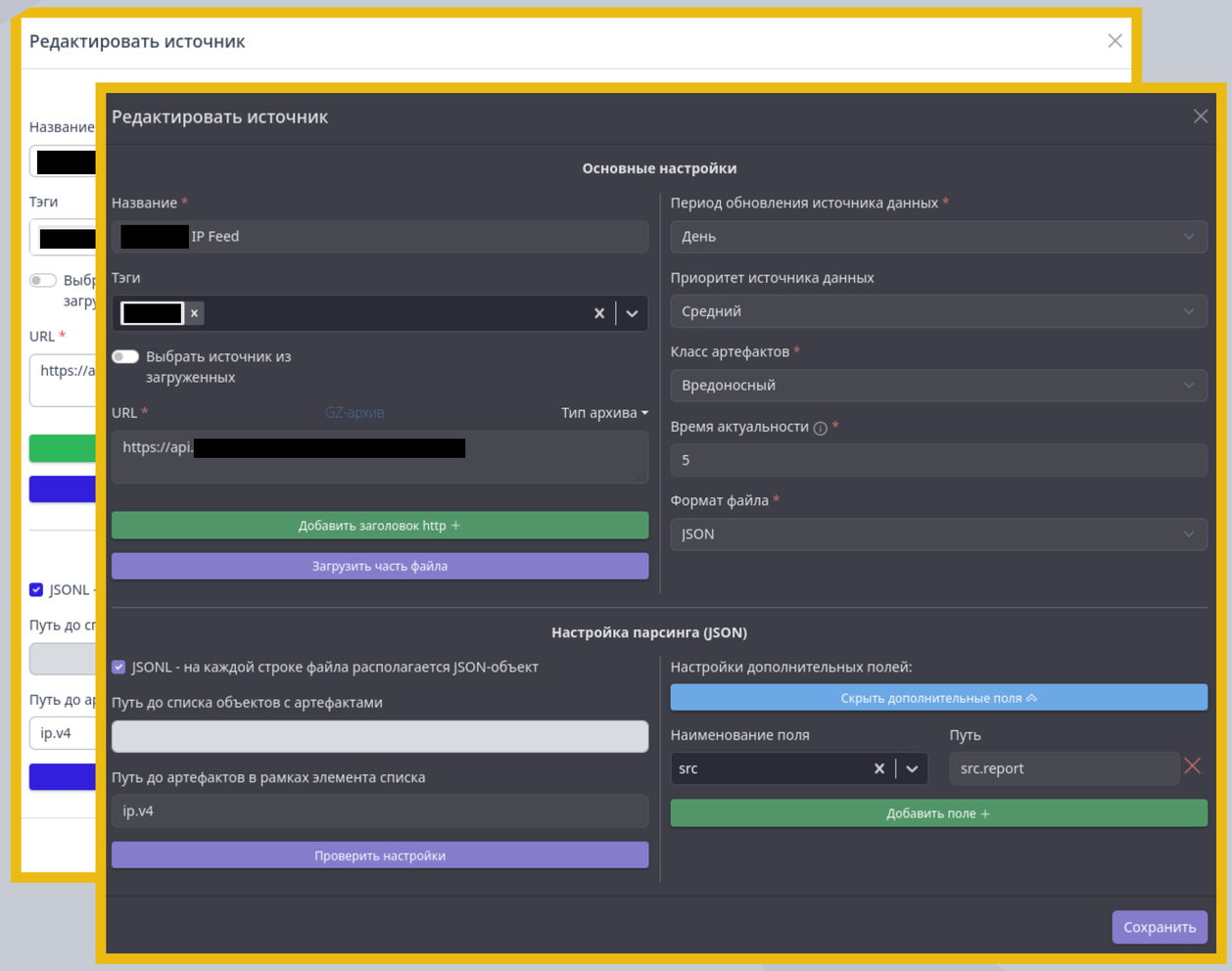


PT
Информационная безопасность

Brick 2

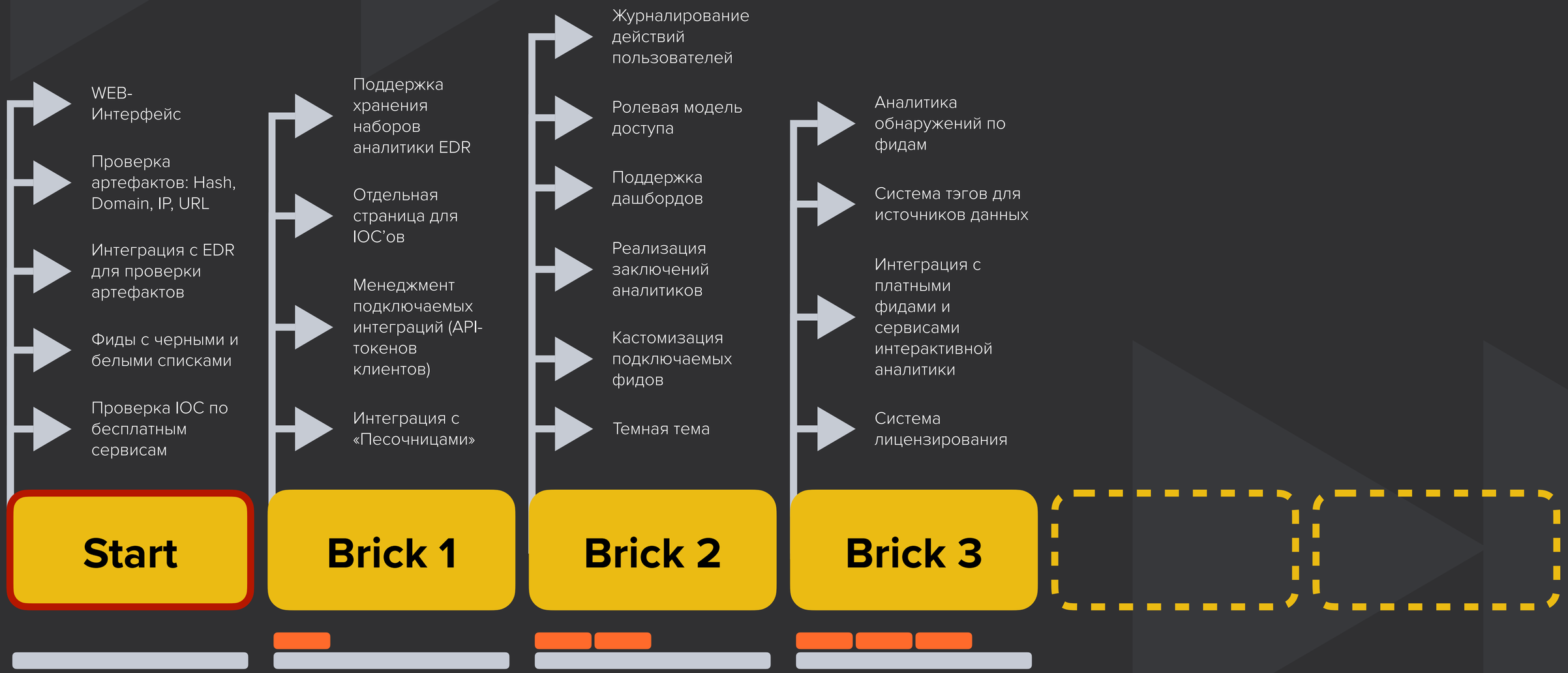
- Поддержка заключения аналитиков
- Кастомизация подключаемых фидов





Brick 3

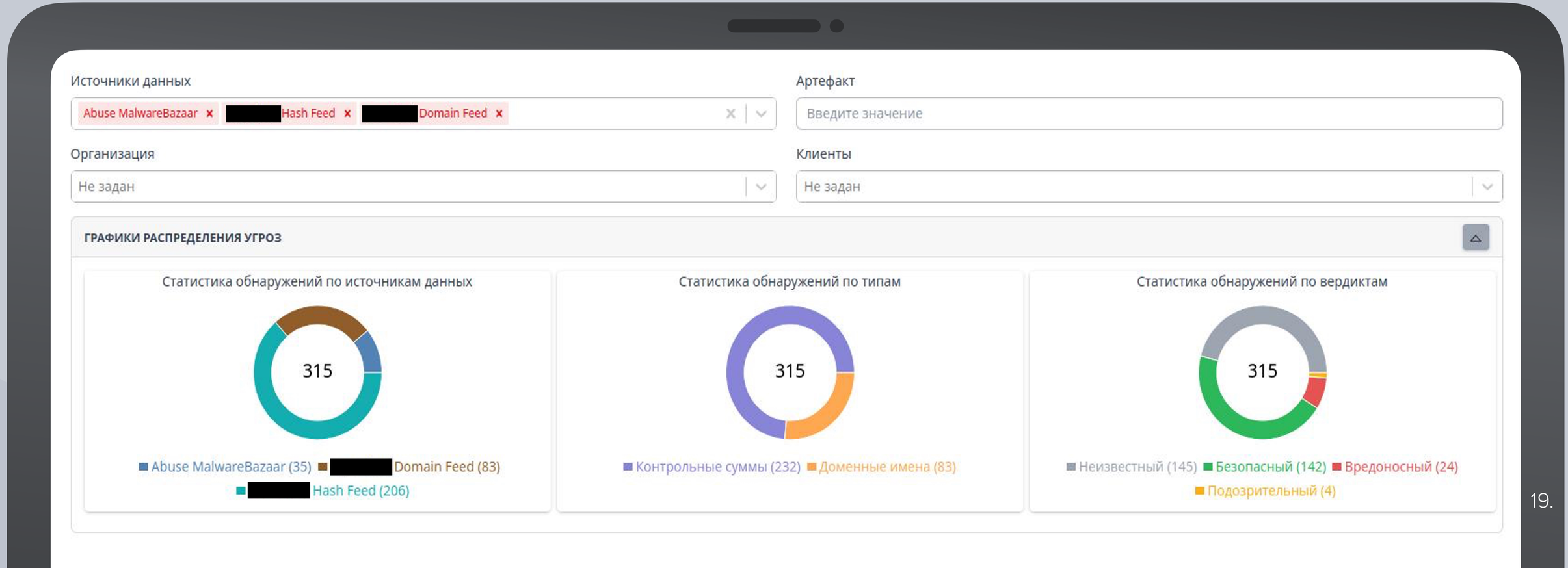
PT
Информационная безопасность



Brick 3

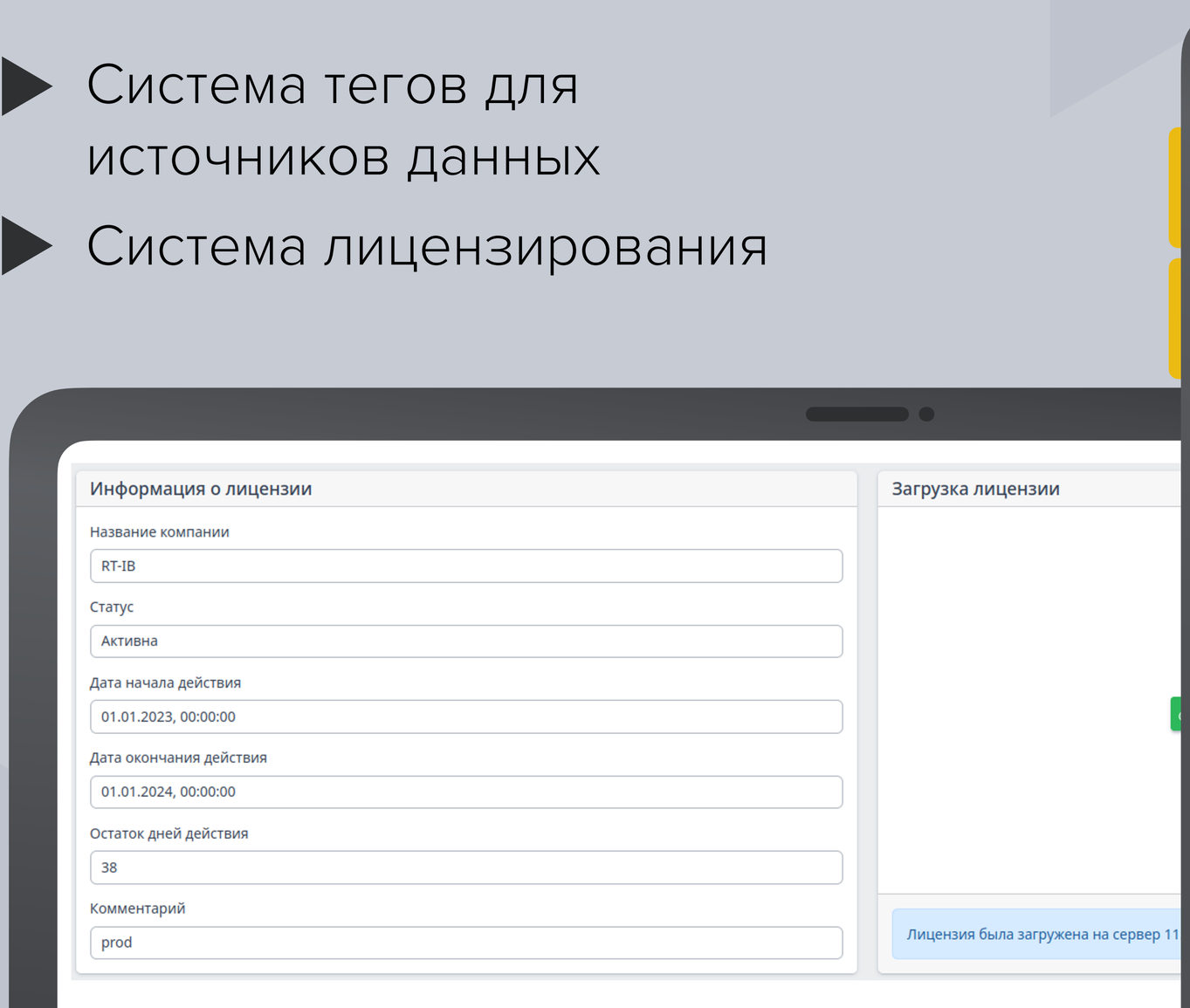
PT
Информационная безопасность

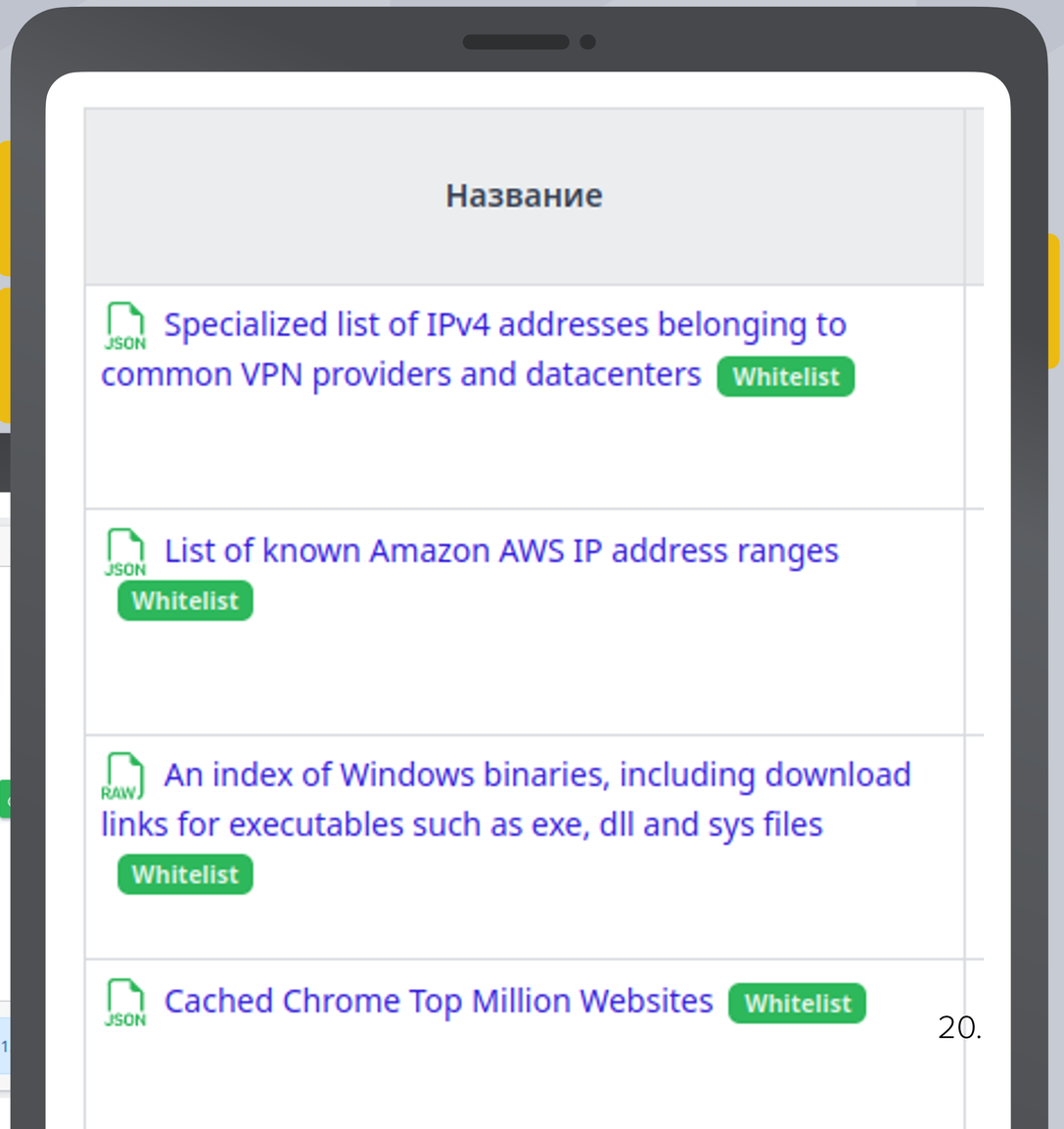
Аналитика обнаружений по фидам и онлайн-сервисам



Brick 3

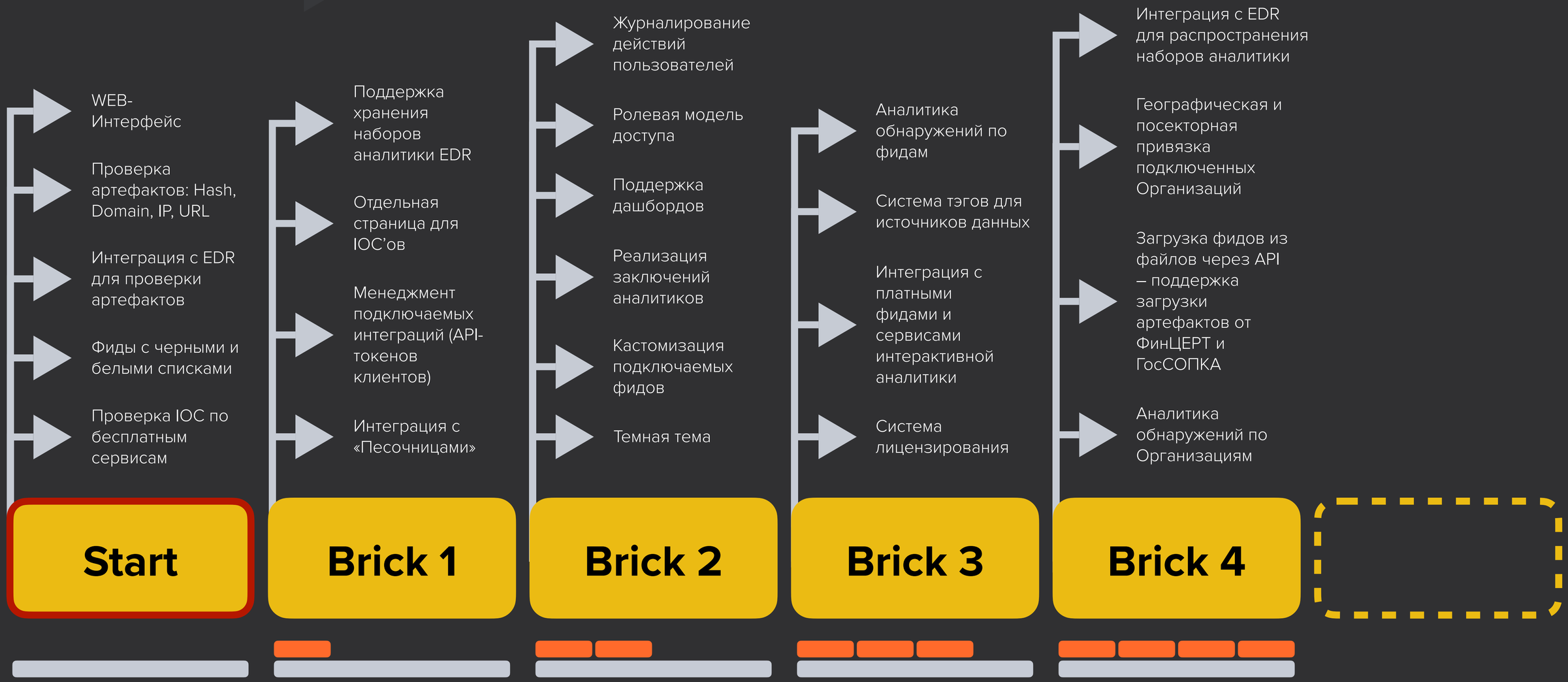
- Система тегов для источников данных
- Система лицензирования





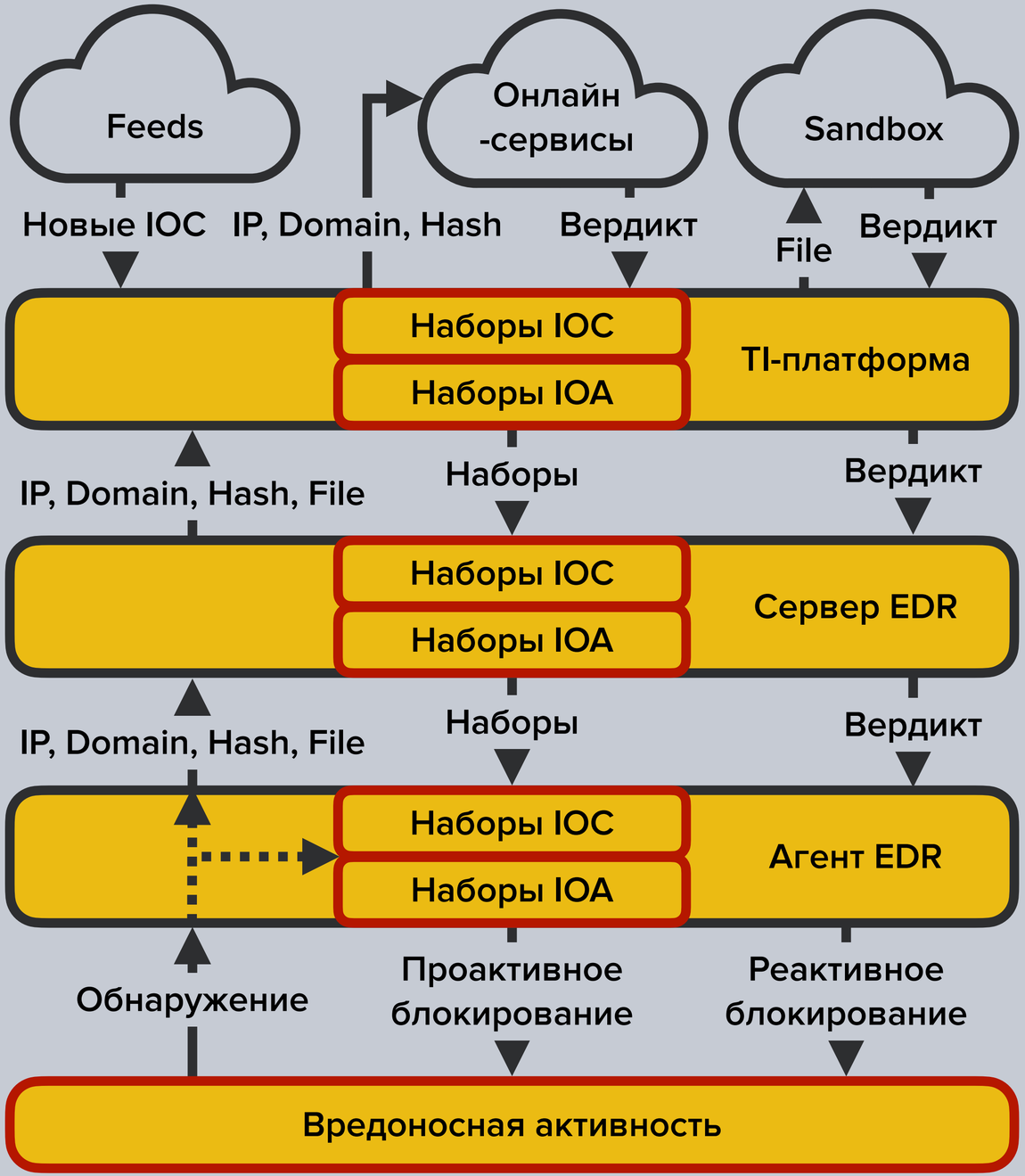
Закончим первый ряд?

PT
Информационная безопасность



Расширение интеграции с EDR

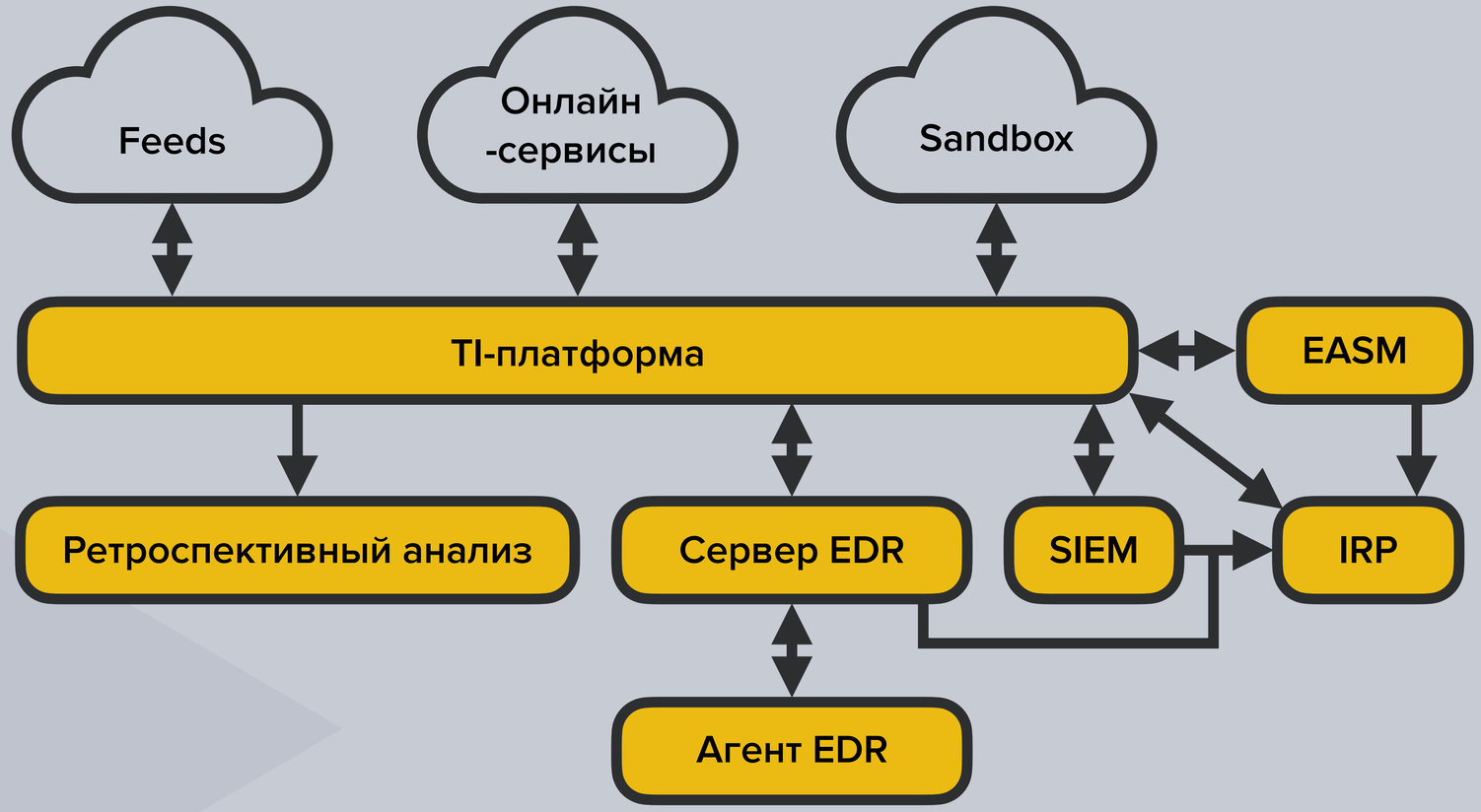
- Распространение наборов IOC и IOA
- Автоматизирована работа со аналитикой множества серверов EDR
- Аналитика обнаружений с каждого сервера



PT
Информационная безопасность

Вклад TI в SOC

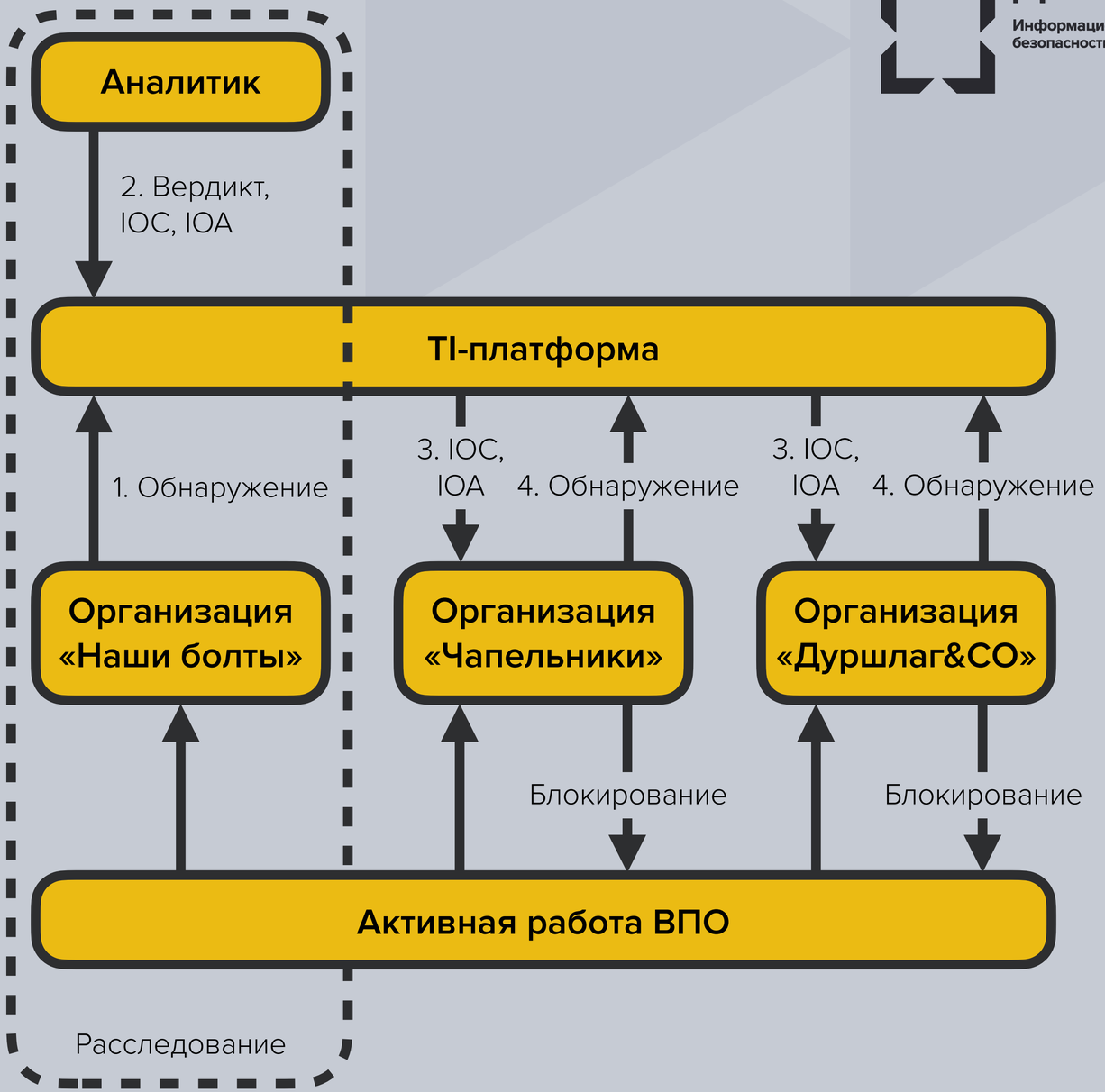
- Распространение наборов аналитики EDR
- Углубление интеграции со всеми процессами



PT
Информационная
безопасность

Практические результаты

- Выделение статистики обнаружений по Организациям
- Ретроспективный поиск по IOC’ам
- Как результат, обнаружение множественных атак на ключевые Организаций



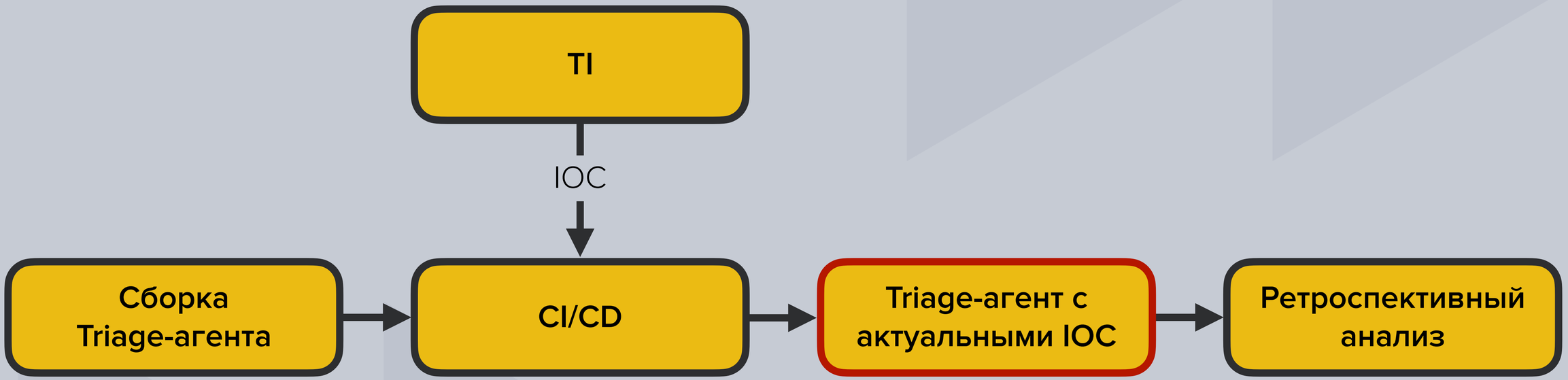
Топ фидов по вкладу в аналитику

- Белые и черные списки:
  - misp-warninglists
  - Платные фиды
  - cinsscore.com
  - winbindex
  - lists.blocklist.de
  - и др.
- Ведется оценка дополнительных общедоступных и проприетарных поставщиков данных TI

PT
Информационная безопасность

Ретроспективный анализ и TI

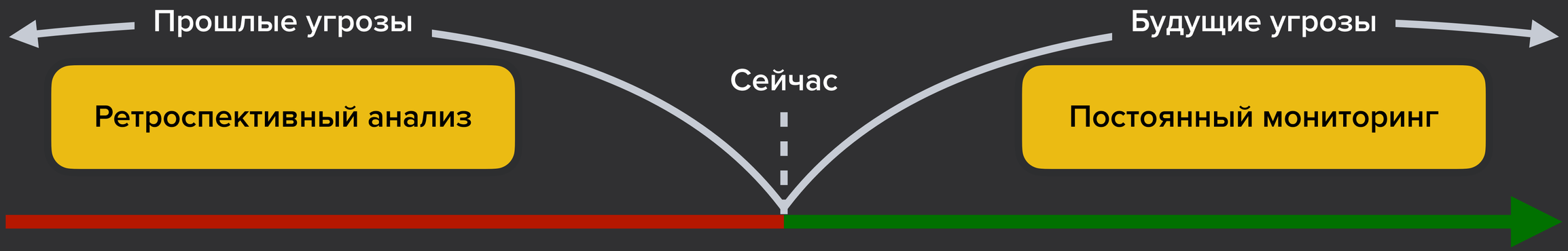
Поставка актуальных индикаторов компрометации
при ретроспективном анализе



PT
Информационная безопасность

Ретроспективный анализ vs мониторинг

- Использование данных об актуальных угрозах с TI
- Проактивно – EDR, ретроспективно – Ретро
- Процесс анализа: сначала ретро, потом мониторинг



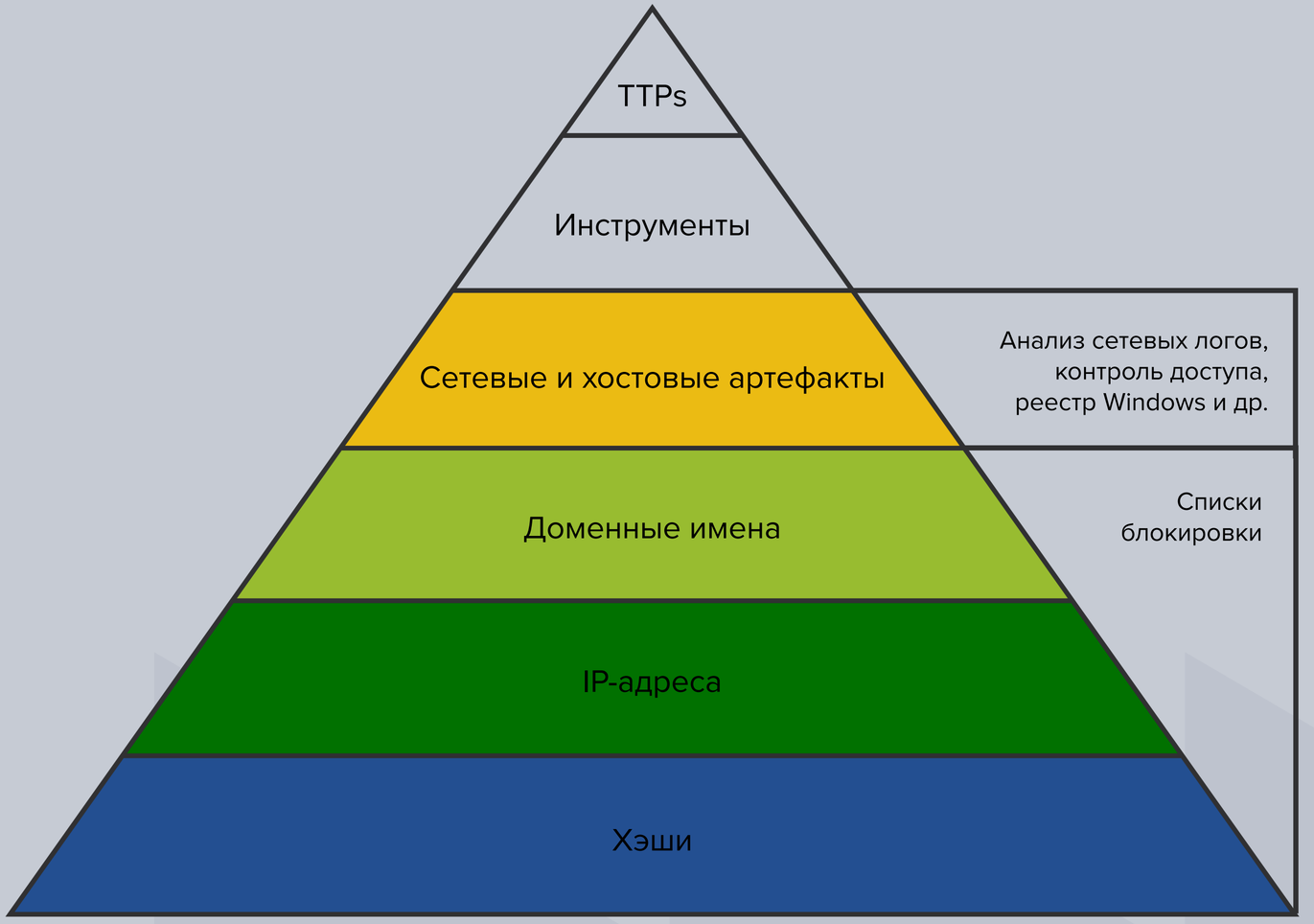
PT
Информационная безопасность

Развитие TI

PT
Информационная безопасность

Полученные результаты

- Стратегический
- Тактический
- Оперативный
- Технический



Что строим дальше?

PT
Информационная безопасность

Что дальше?

Анализ сущностей APT, Campaign и др, корреляция техник Mitre, анализ DarkWeb, OSINT и многое другое

Поддержка Threat Exchange протоколов

Переход на более высокие уровни аналитики

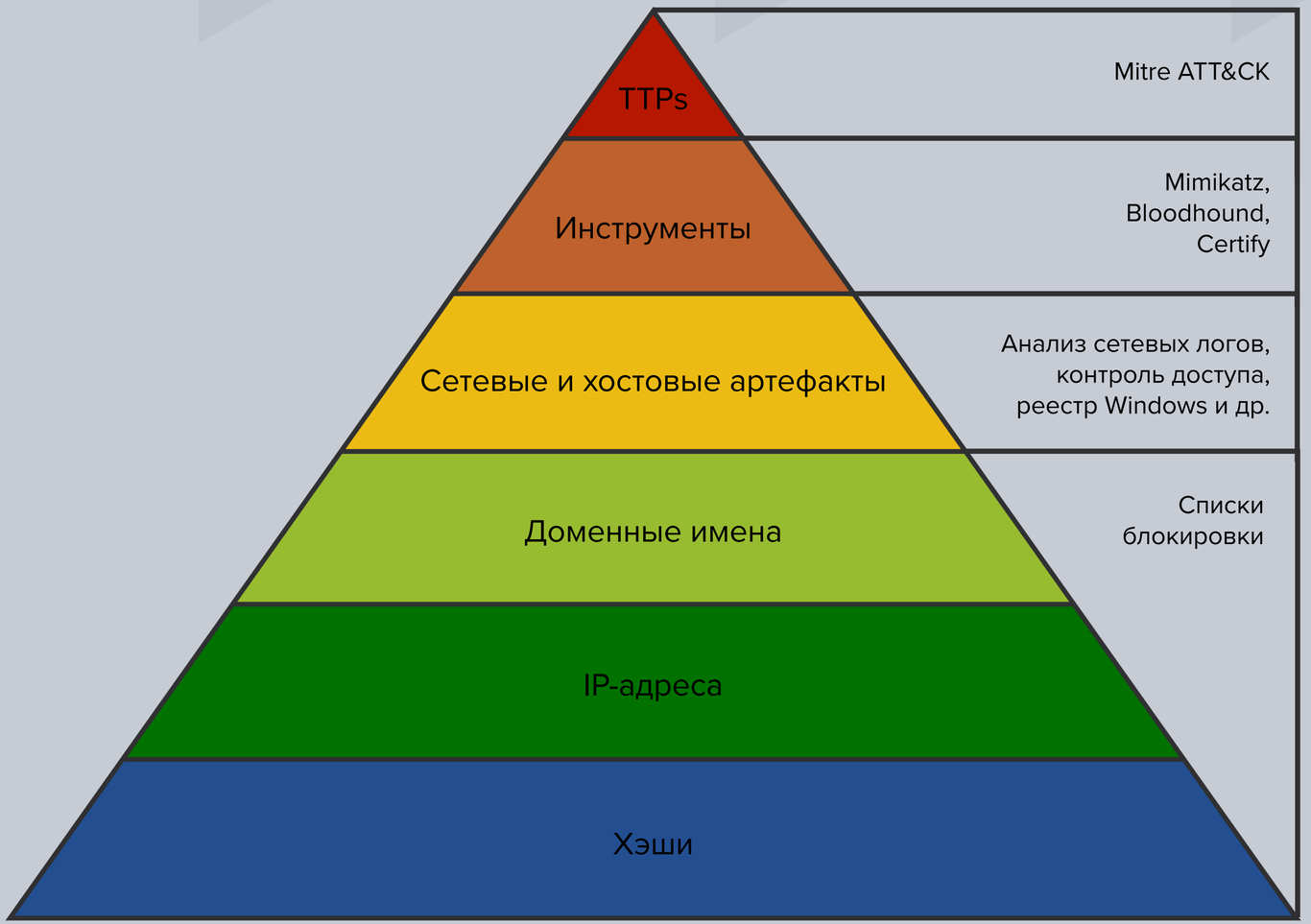
PT
Информационная безопасность

Потенциальный результат

PT
Информационная безопасность

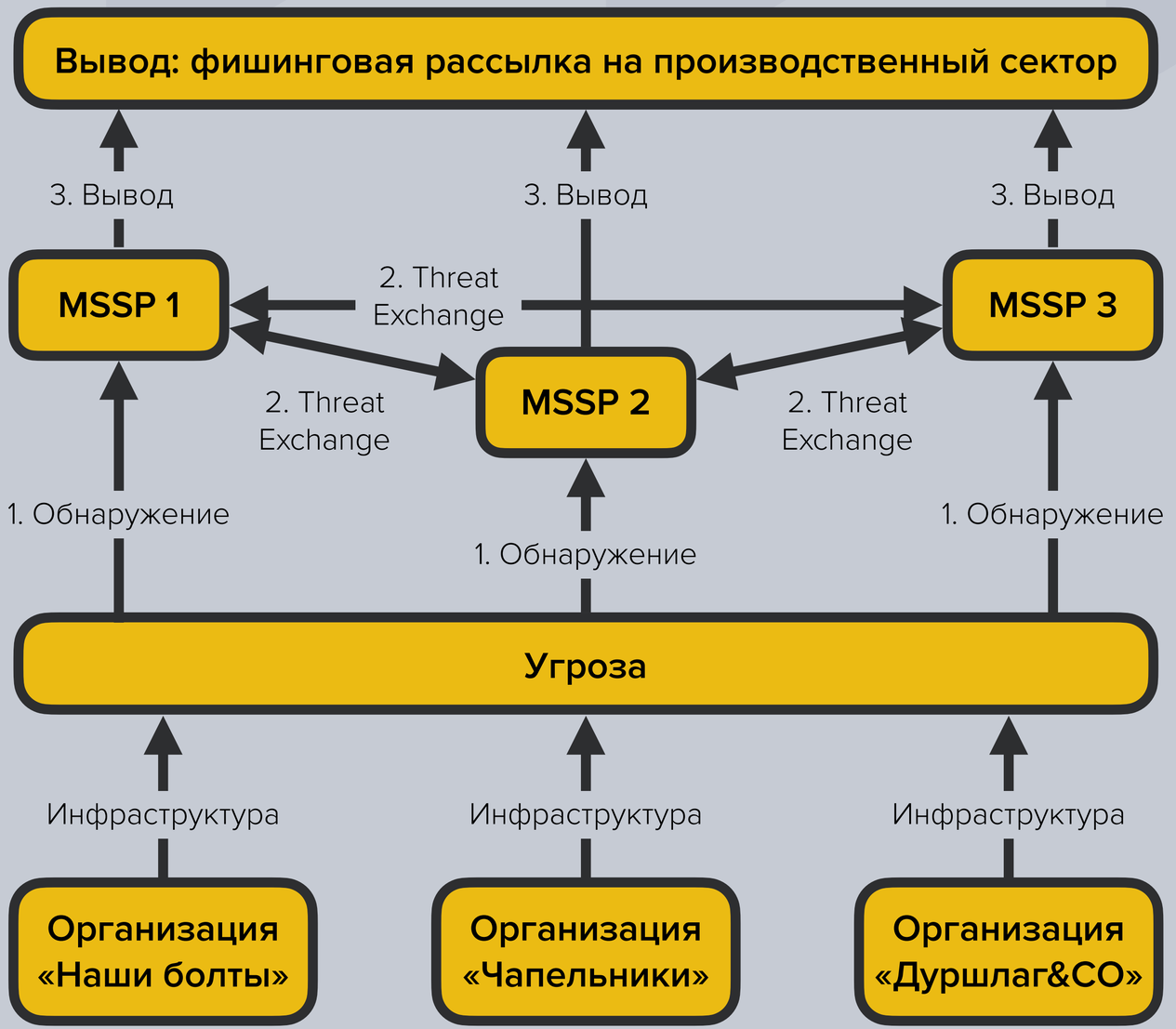
Глобальная система разведки угроз

- Стратегический
- Тактический
- Оперативный
- Технический



Как обеспечить глобальную систему реагирования?

- Обмен в рамках отрасли данными об угрозах
- Переход от реагирования в рамках ИБ-компаний к глобальному реагированию
- Collective Defence Intelligence
- Прогнозирование угроз/ атак



Нам доверяют

Ростех
РТ-Энергоэффективность

РТ
Развитие бизнеса

Ростех
Техприемка

Ростех

KAMAZ

ОАК
Объединенная авиастроительная корпорация

ОДК

КБП

СИБЕР

Нацимбио

Высокоточные комплексы

УВЗ

Акционерное общество
Рязанский радиозавод

Контакты

Адрес: 117587, г. Москва,
Варшавское шоссе,
дом 118, корпус 1

Tel.: +7 (499) 390-79-05

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru

РТ
Информационная безопасность