

RT
Protect TI

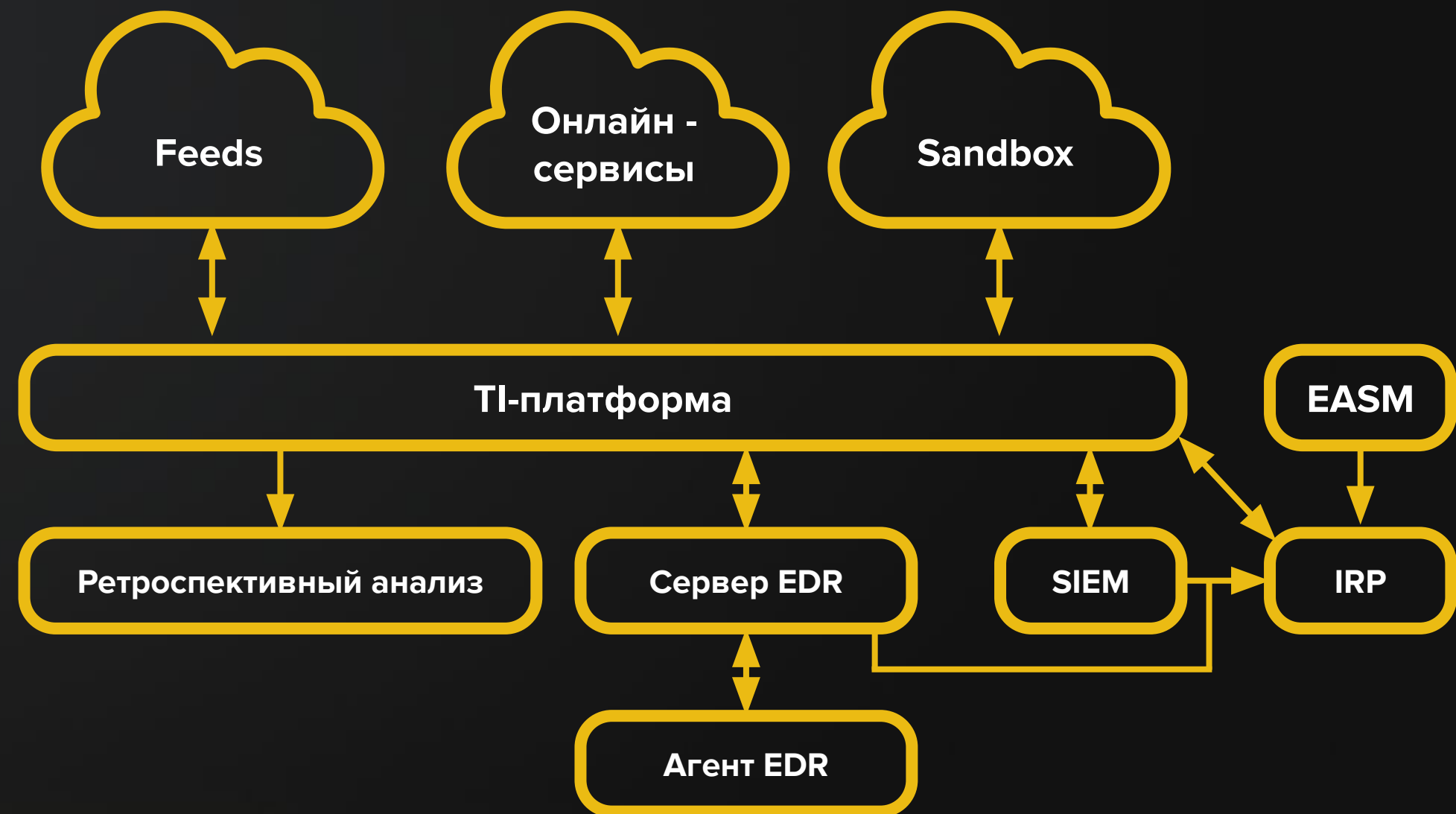


RT Protect TI

RT Protect TI

– платформа, предоставляющая функционал по агрегации, корреляции и хранению данных о киберугрозах, обеспечению своевременности мер реагирования, а также актуализации экспертизы.

- ▶ Определение мотивов, целей, тактик и техник атакующих
- ▶ Актуализация экспертизы
- ▶ Пополнение базы знаний об актуальных угрозах
- ▶ Анализ угроз, зафиксированных в инфраструктуре Заказчиков
- ▶ Обогащение при расследовании инцидентов
- ▶ Распространение наборов аналитики EDR
- ▶ Углубление интеграции со всеми процессами
- ▶ Основа реагирования – **EDR**
- ▶ Приоритет: **проактивная защита**



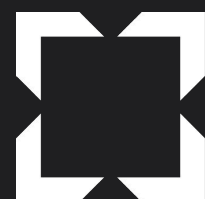
Вокруг чего выстраивать процессы TI?



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



Настройка фидов

- ▶ Поддержка заключения аналитиков
- ▶ Кастомизация подключаемых фидов

Добавить заключение аналитика

Вердикт *

Вредоносный

Комментарий *

По результатам анализа данный файл признан вредоносным.

Время актуальности *

Бесконечно

Добавить

Редактировать источник

Название

Тэги

Выбор загрузки

URL *

https://api.

URL *

https://api.

Путь до списка объектов с артефактами

Путь до артефактов в рамках элемента списка

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

Редактировать источник

Основные настройки

Название *

IP Feed

Тэги

Выбор источника из загруженных

URL *

URL *

https://api.

Путь до списка объектов с артефактами

Путь до артефактов в рамках элемента списка

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

Добавить заголовок http +

Загрузить часть файла

Проверить настройки

Настройка парсинга (JSON)

JSONL - на каждой строке файла располагается JSON-объект

Путь до списка объектов с артефактами

Путь до артефактов в рамках элемента списка

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

ip.v4

Период обновления источника данных *

День

Приоритет источника данных

Средний

Класс артефактов *

Вредоносный

Время актуальности ① *

5

Формат файла *

JSON

Настройки дополнительных полей:

Скрыть дополнительные поля

Наименование поля

src

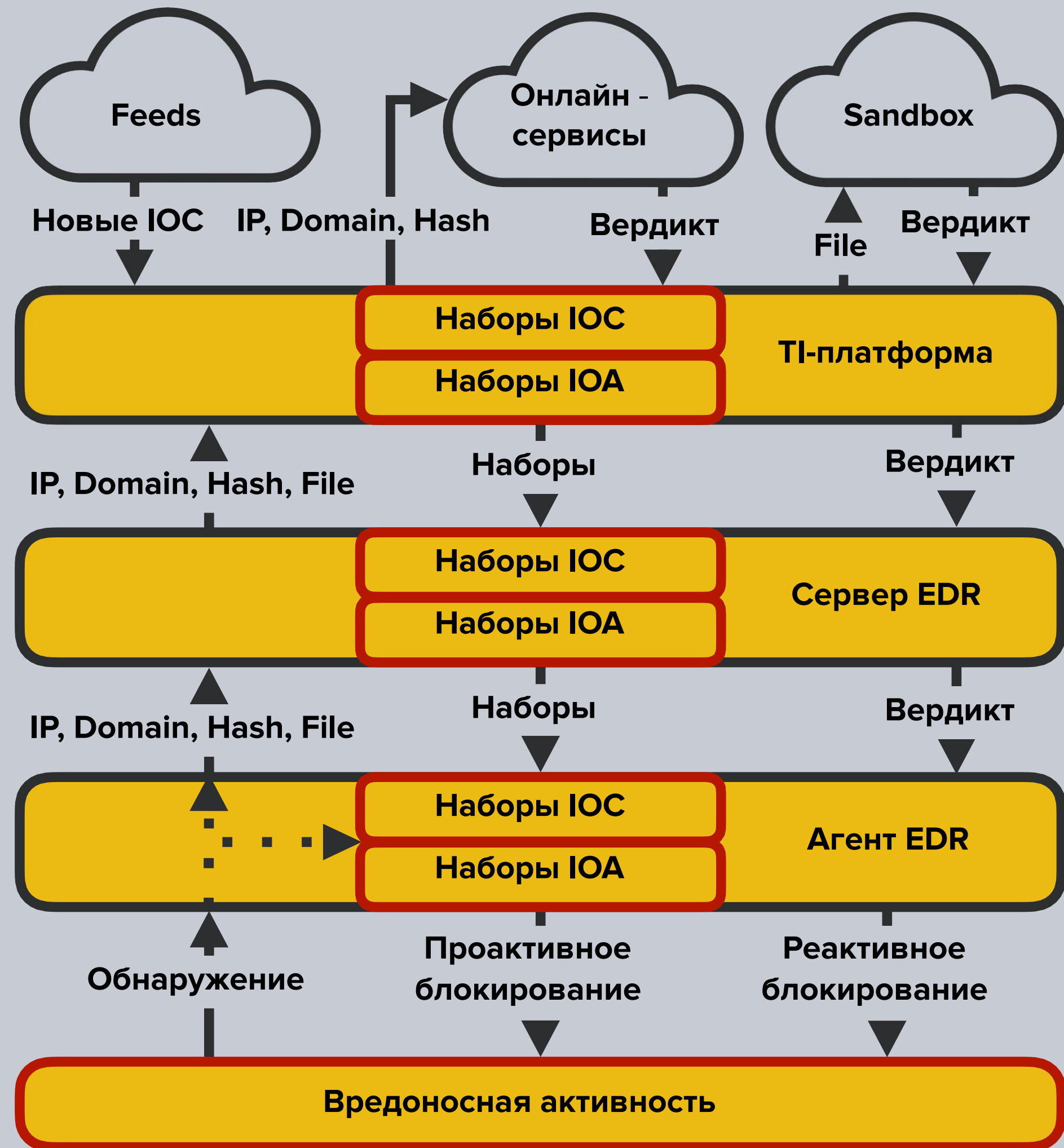
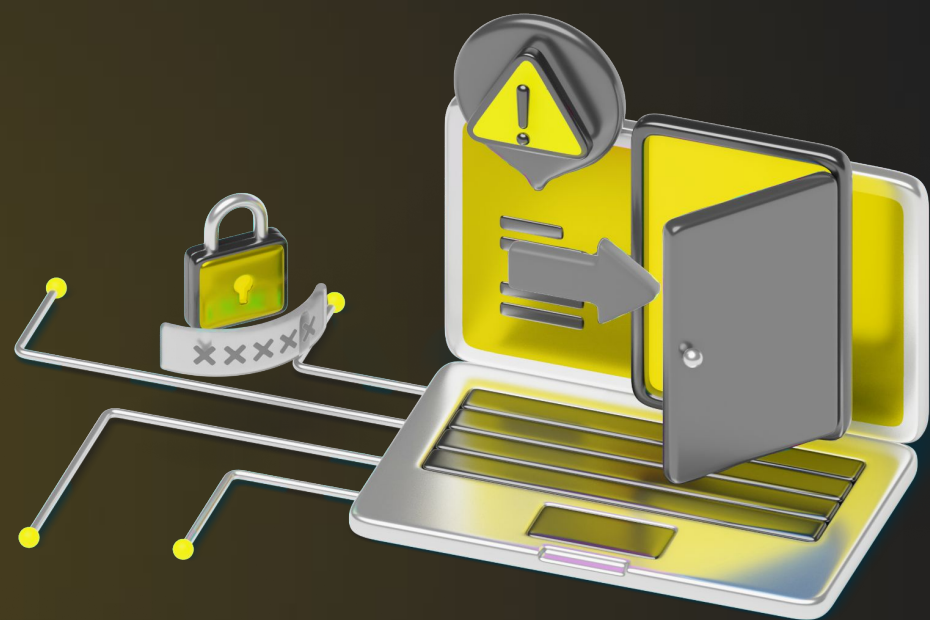
src.report

Добавить поле +

Сохранить

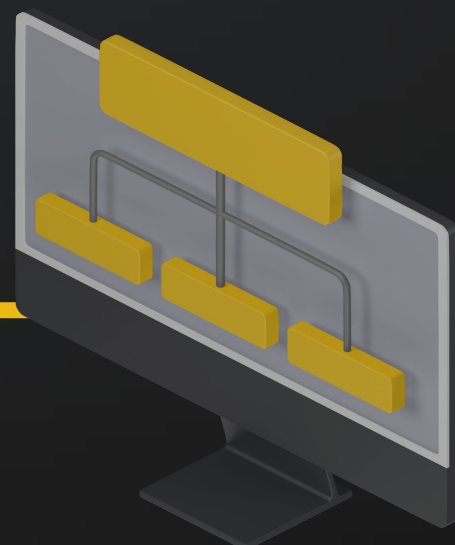
Глубокая интеграция с EDR

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



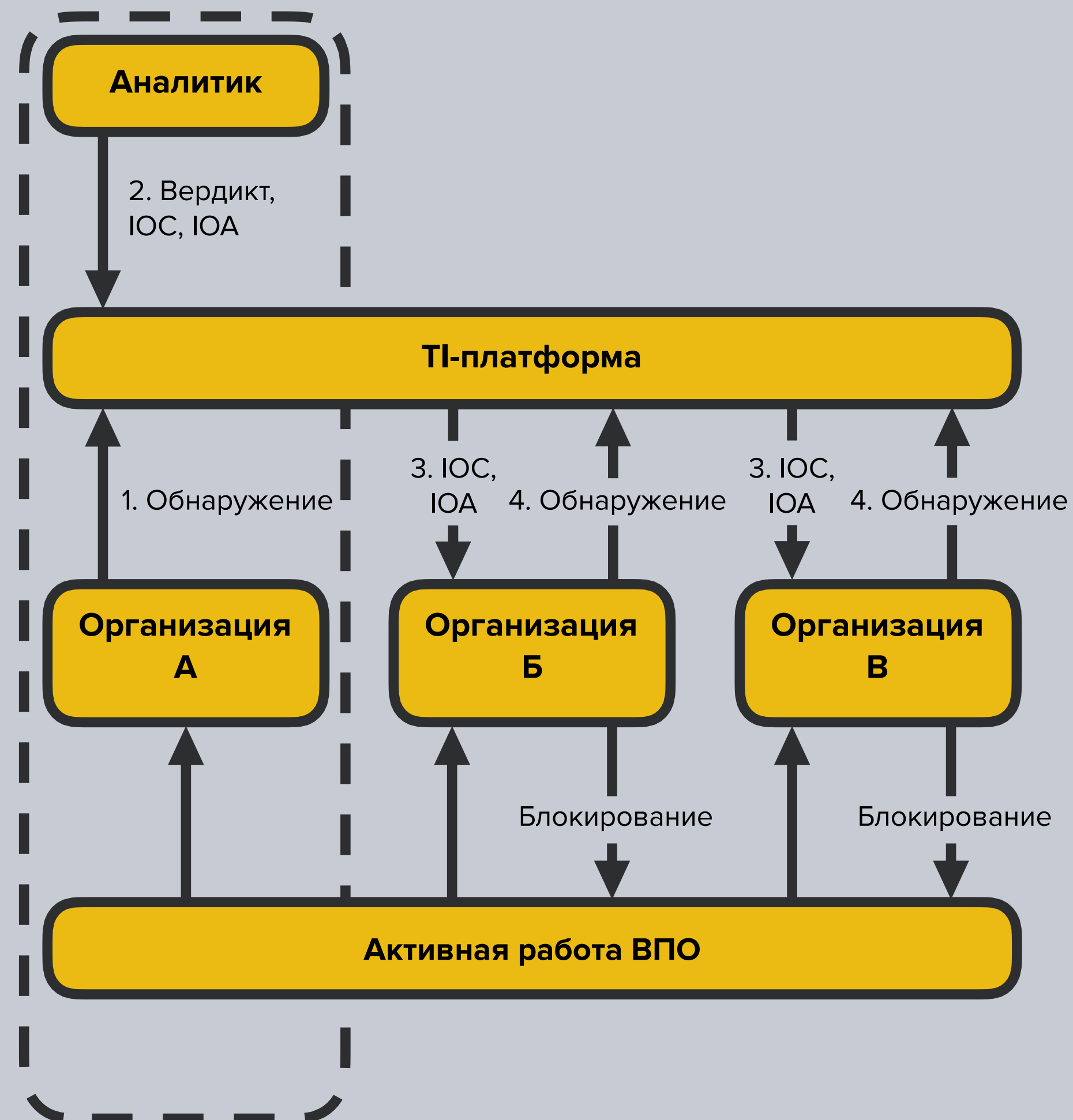
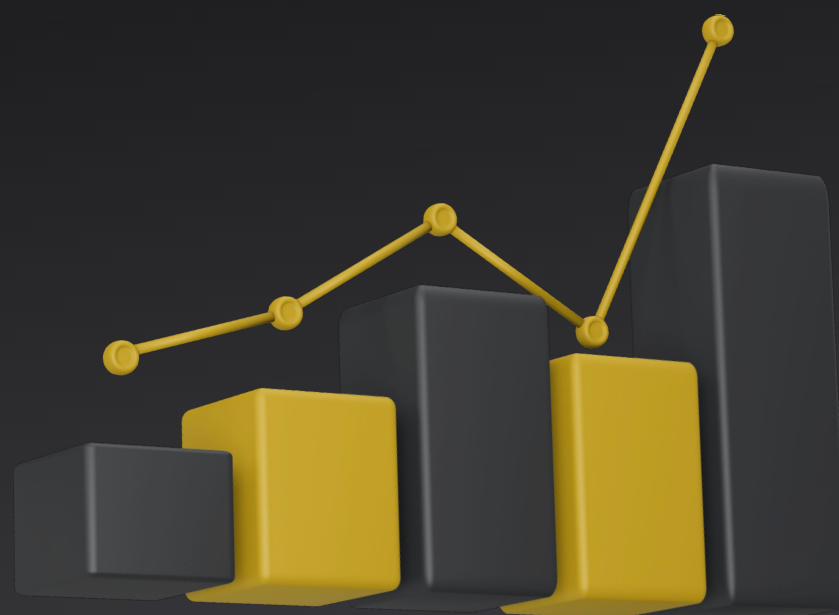
Граф связей

- Возможность интерактивного построения графа связей артефактов позволяет проводить доскональное расследование инцидентов и активно использовать накопленную базу знаний в дальнейшем



Практические результаты RT Protect TI

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



Дорожная карта разработки



Нам доверяют



КБП



СИБЕР

Нацимбио



НОВИКОМБАНК

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

