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**

PT
Информационная безопасность

Вокруг чего выстраивать процессы TI?

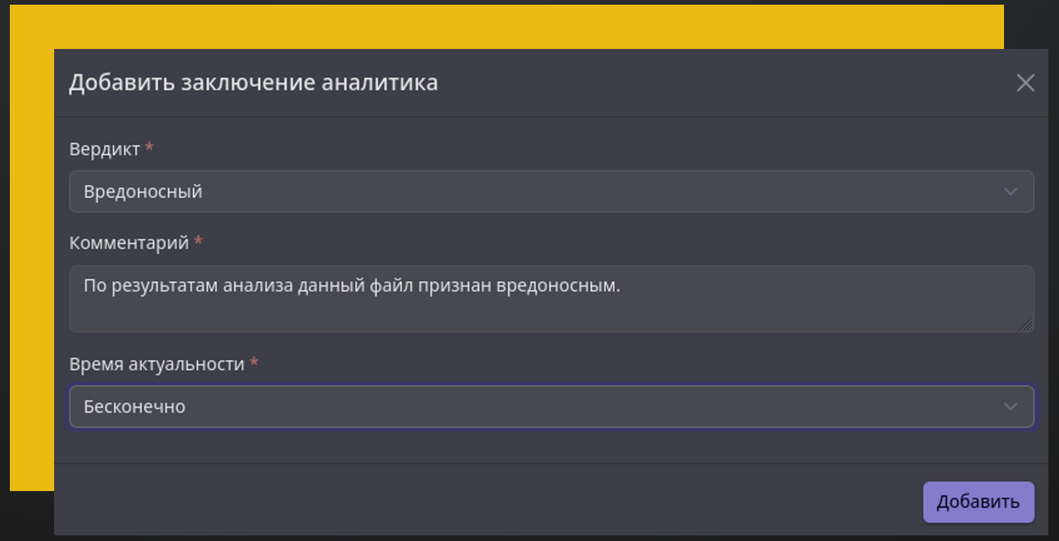
TI-платформа
Основные функции:

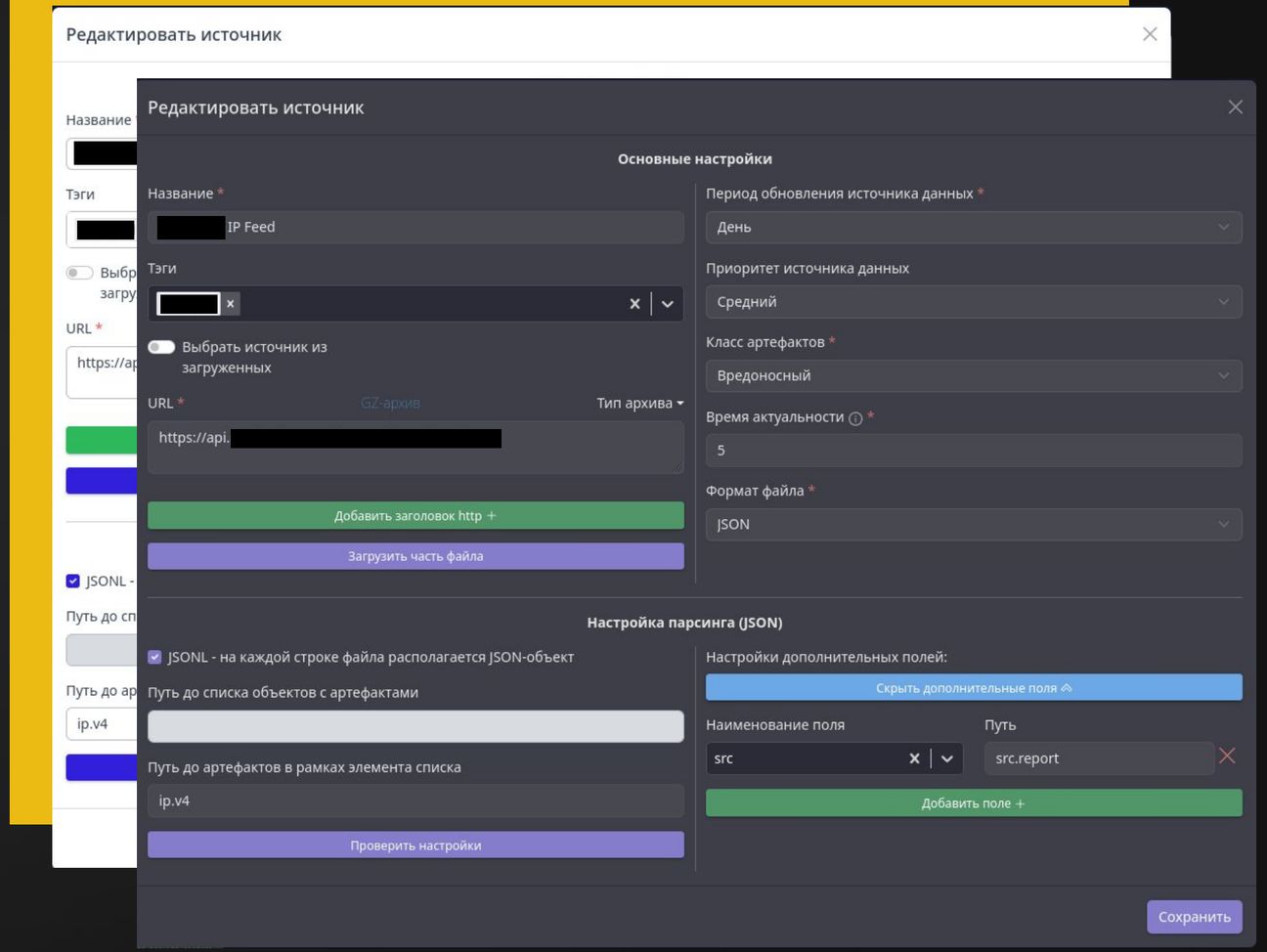
- **Сбор и анализ данных из фидов** (TI Feeds)
- Интеграции со сторонними сервисами (VT, решения класса Sandbox и т.д.)
- Применение IOC и IOA в EDR для активной блокировки угроз
- Обогащение данных событий, инцидентов
- Аналитика угроз

PT
Информационная безопасность

Настройка фидов

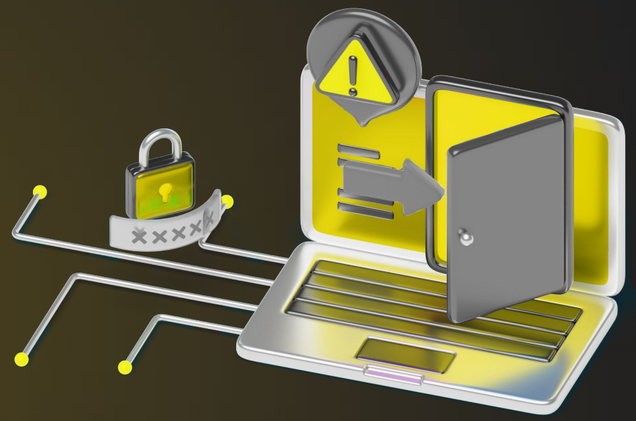
- Поддержка заключения аналитиков
- Кастомизация подключаемых фидов



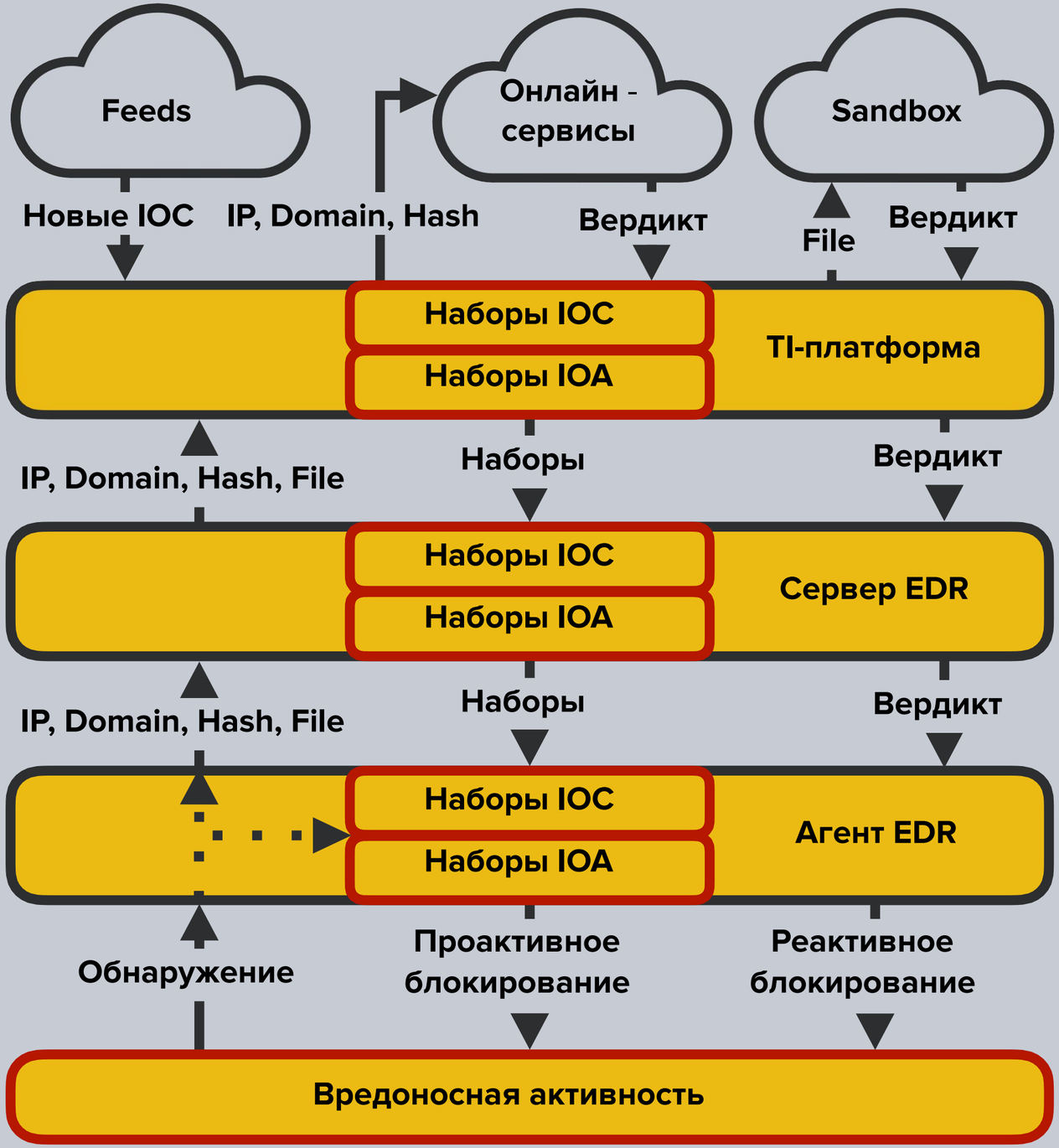


Глубокая интеграция с EDR

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

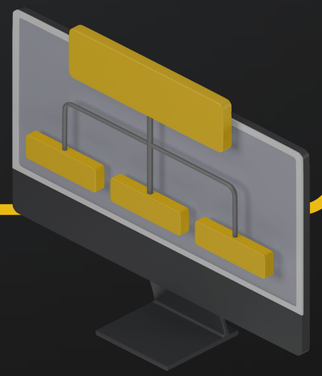


PT
Информационная безопасность



Граф связей

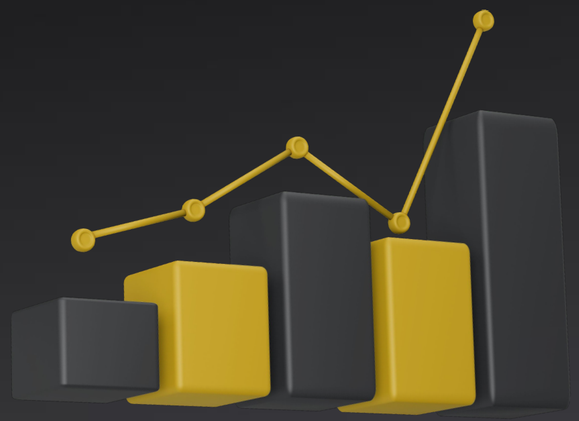
- Возможность интерактивного построения графа связей артефактов позволяет проводить досконально расследование инцидентов и активно использовать накопленную базу знаний в дальнейшем

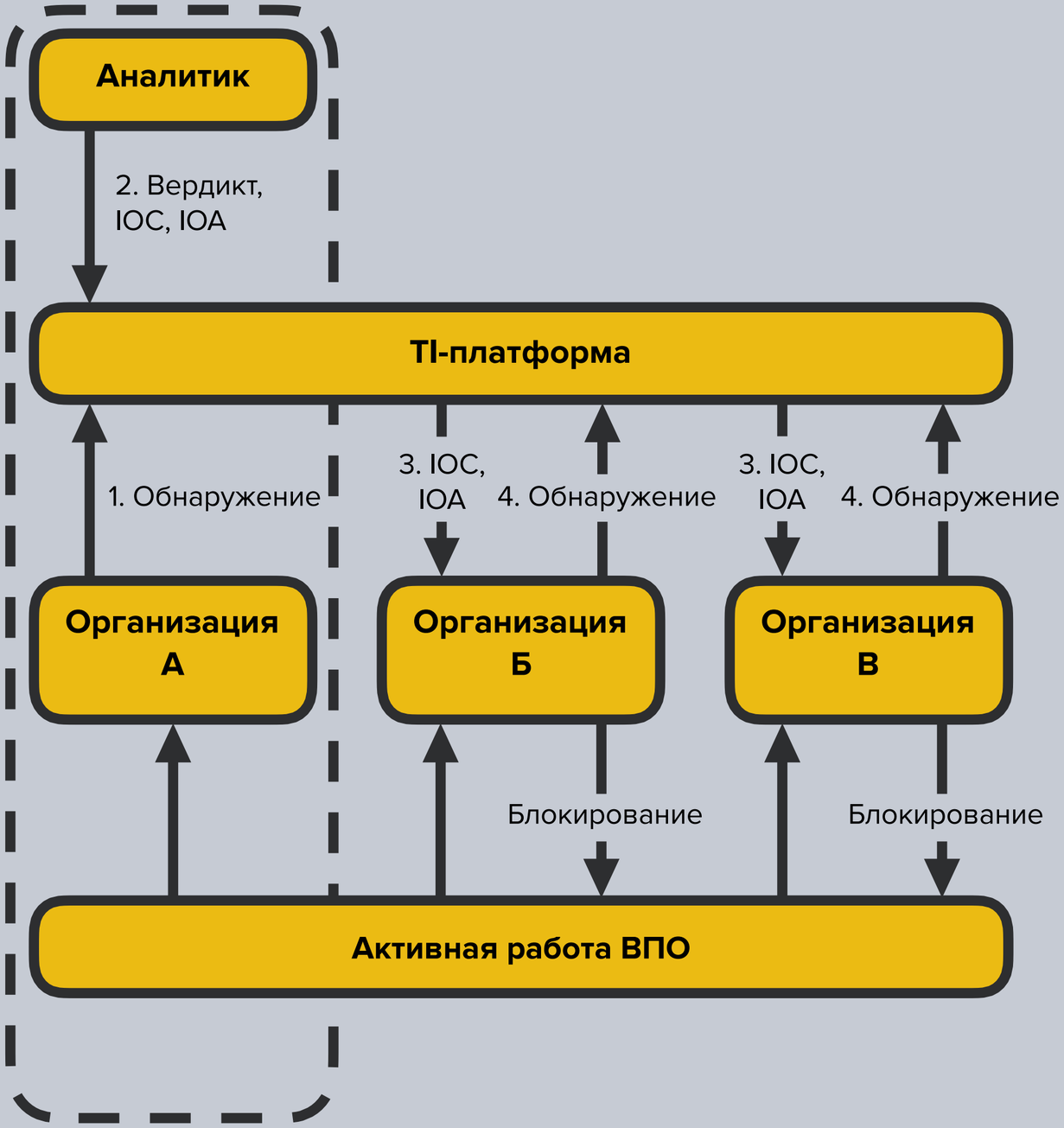


РТ
Информационная безопасность

Практические результаты RT Protect TI

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





RT
Информационная безопасность

Нам доверяют

Ростех
РТ-Энергоэффективность
РТ
Развитие бизнеса
Ростех
Техприемка
Ростех
KAMAZ
ОАК
Объединенная авиастроительная корпорация
ОДК
КБП
СИБЕР
Нацимбио
Высокоточные комплексы
УВЗ
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