R-Vision

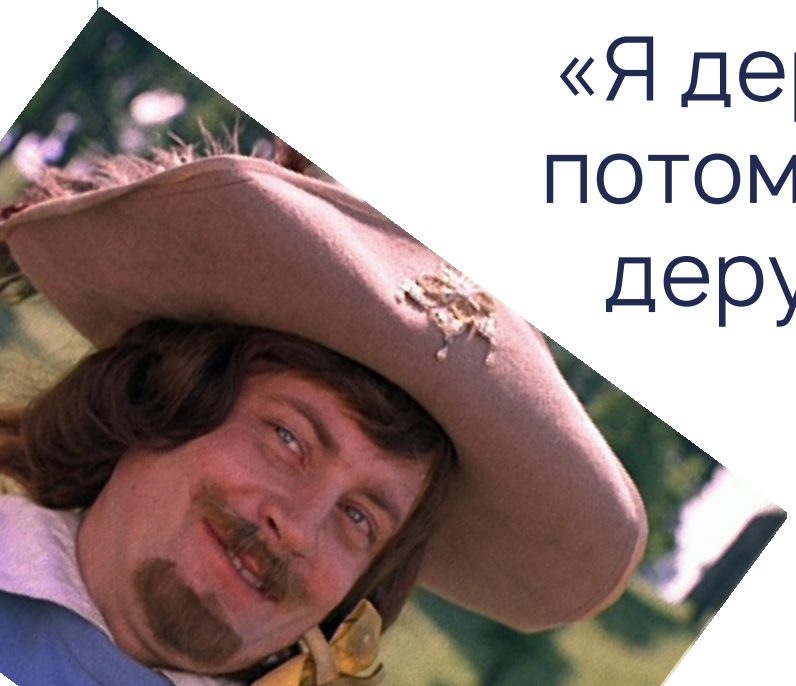
Путь SOC: инциденты и реагирование

Мельшиян Максим
Консультант по ИБ
mmelshiyan@rvision.ru

Зачем реагировать на инциденты?

Нет

«Я дерусь, потому что дерусь»



Да

Снизить риски

Главные вопросы

- Что защищаем?
- С кем сражаемся?
- Что может произойти?
- Как победить?
- Что делать потом?

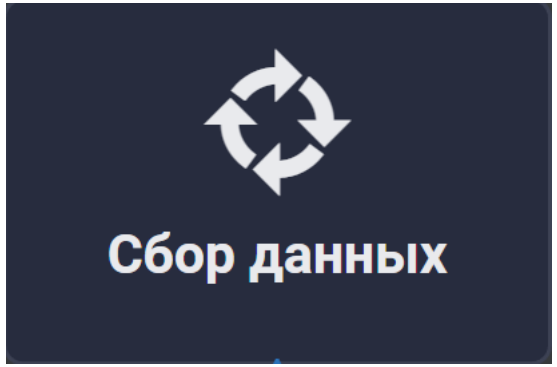
Подготовка

Что защищаем?

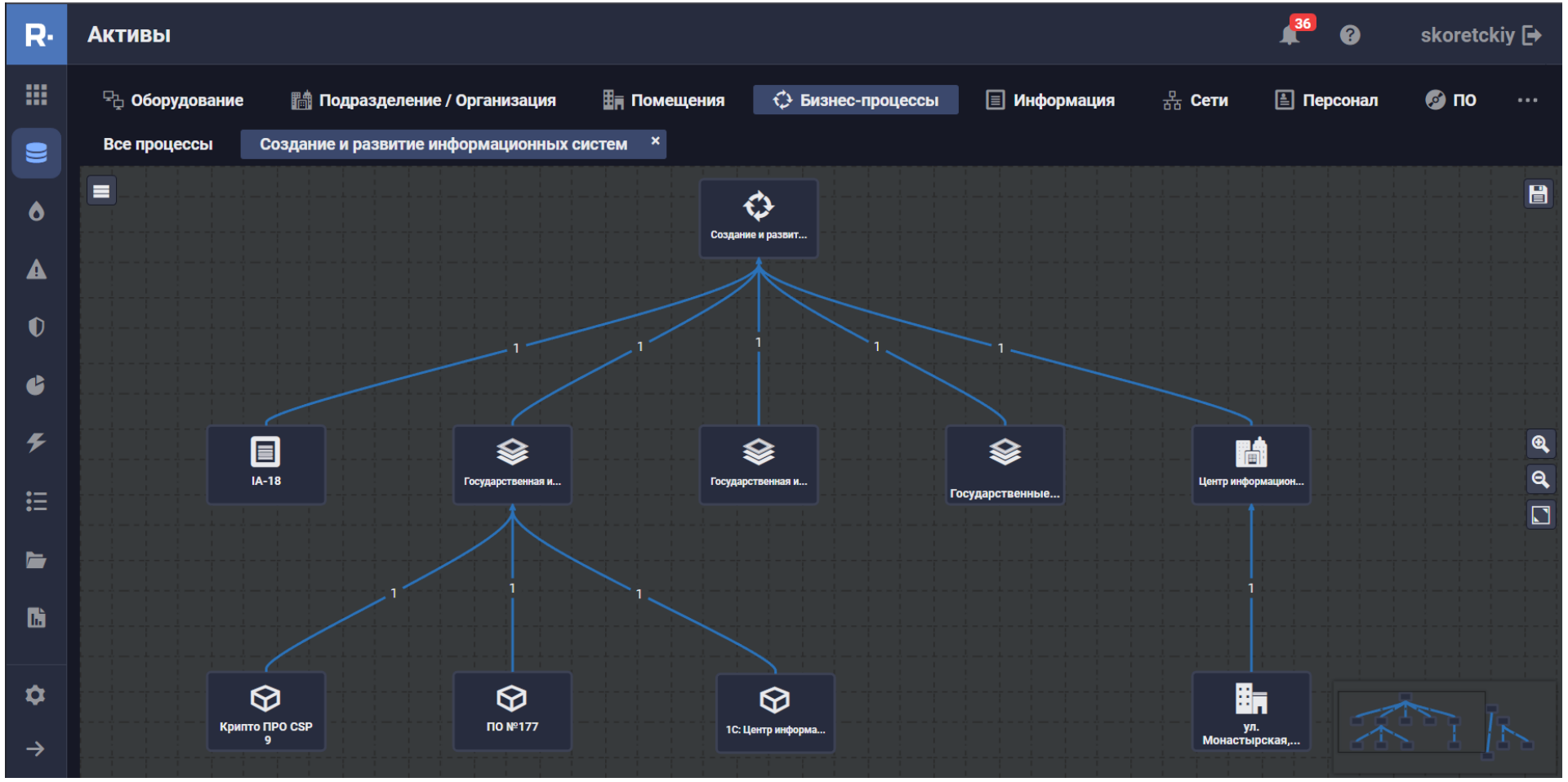
С кем мы сражаемся?

Что может произойти?

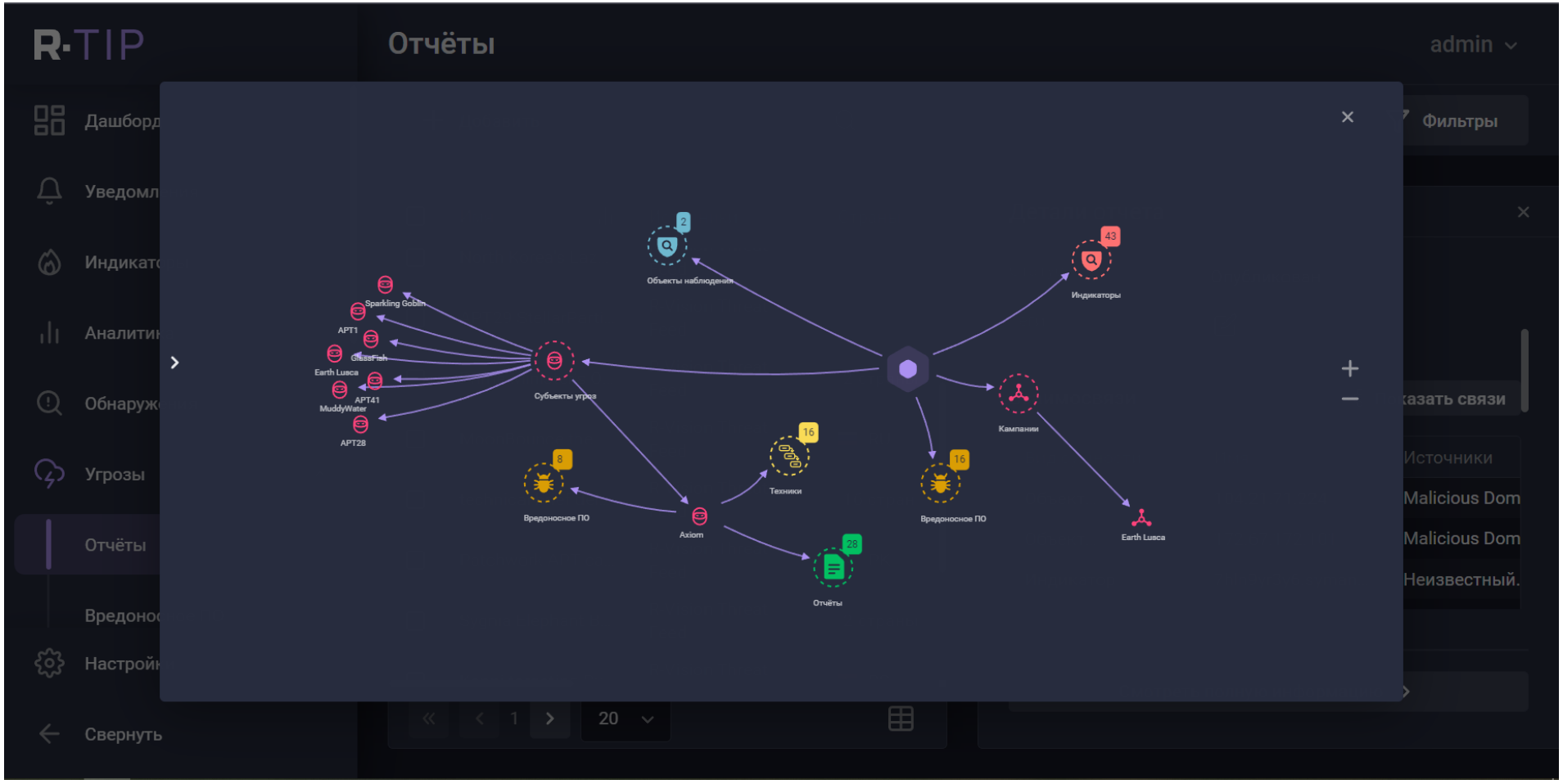
Что защищаем?



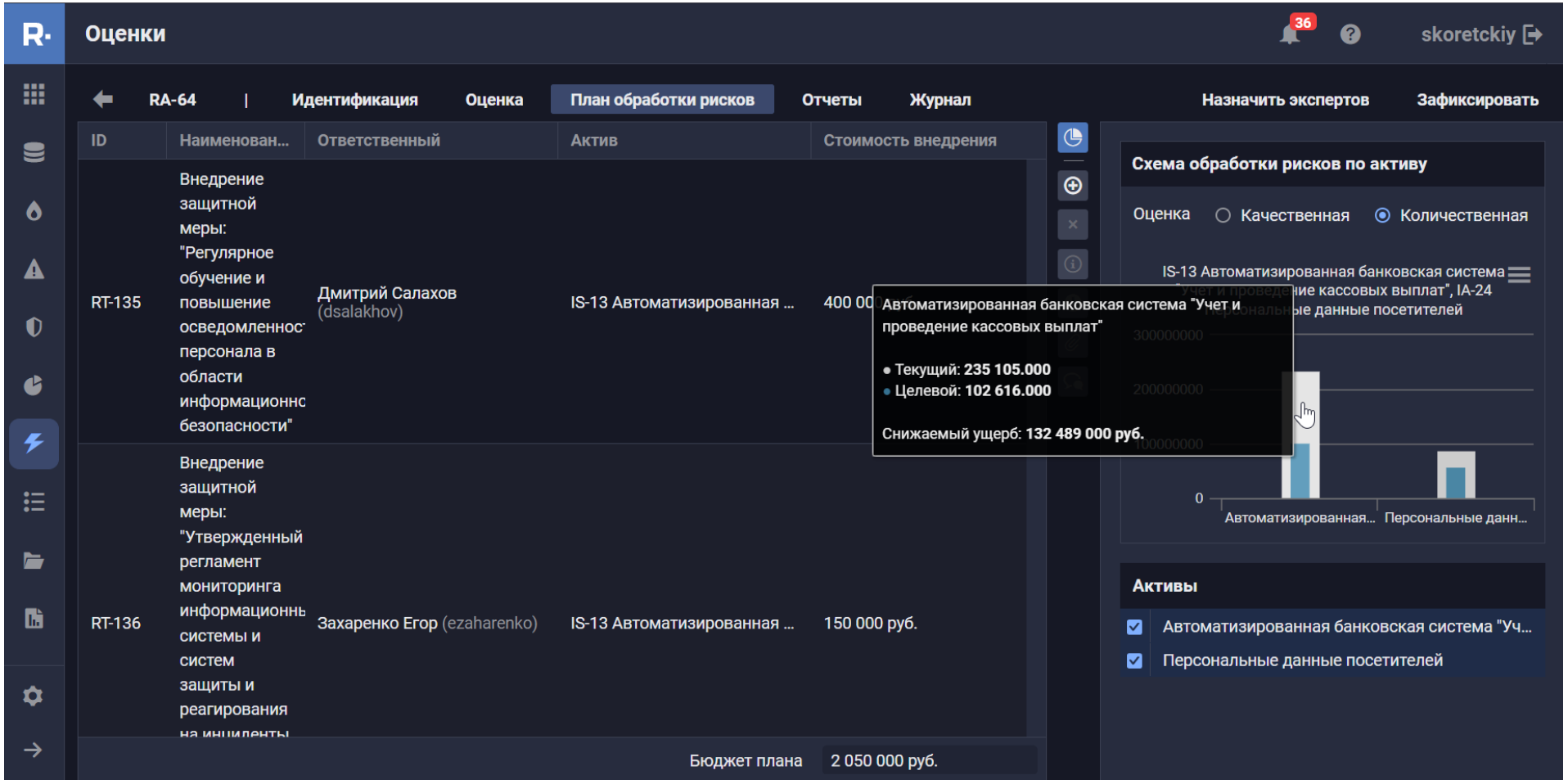
Что защищаем?



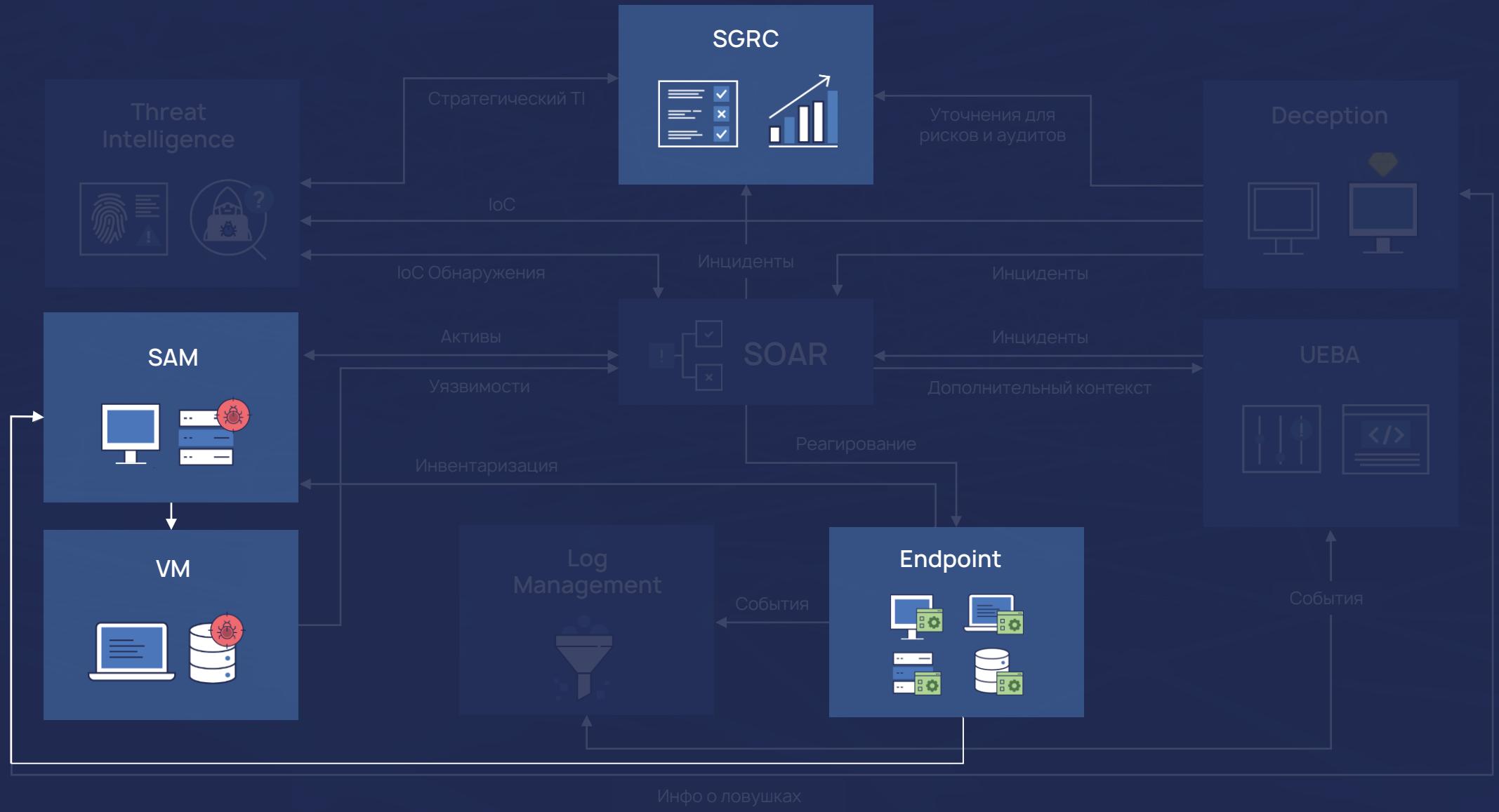
С кем сражаемся?



Что может произойти?



Инвентаризация и стратегия



Обнаружение и реагирование

Как победить?

Как победить?

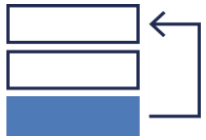
Вектор атаки

Признак инцидента

Источники индикаторов

Анализ инцидента

Документирование



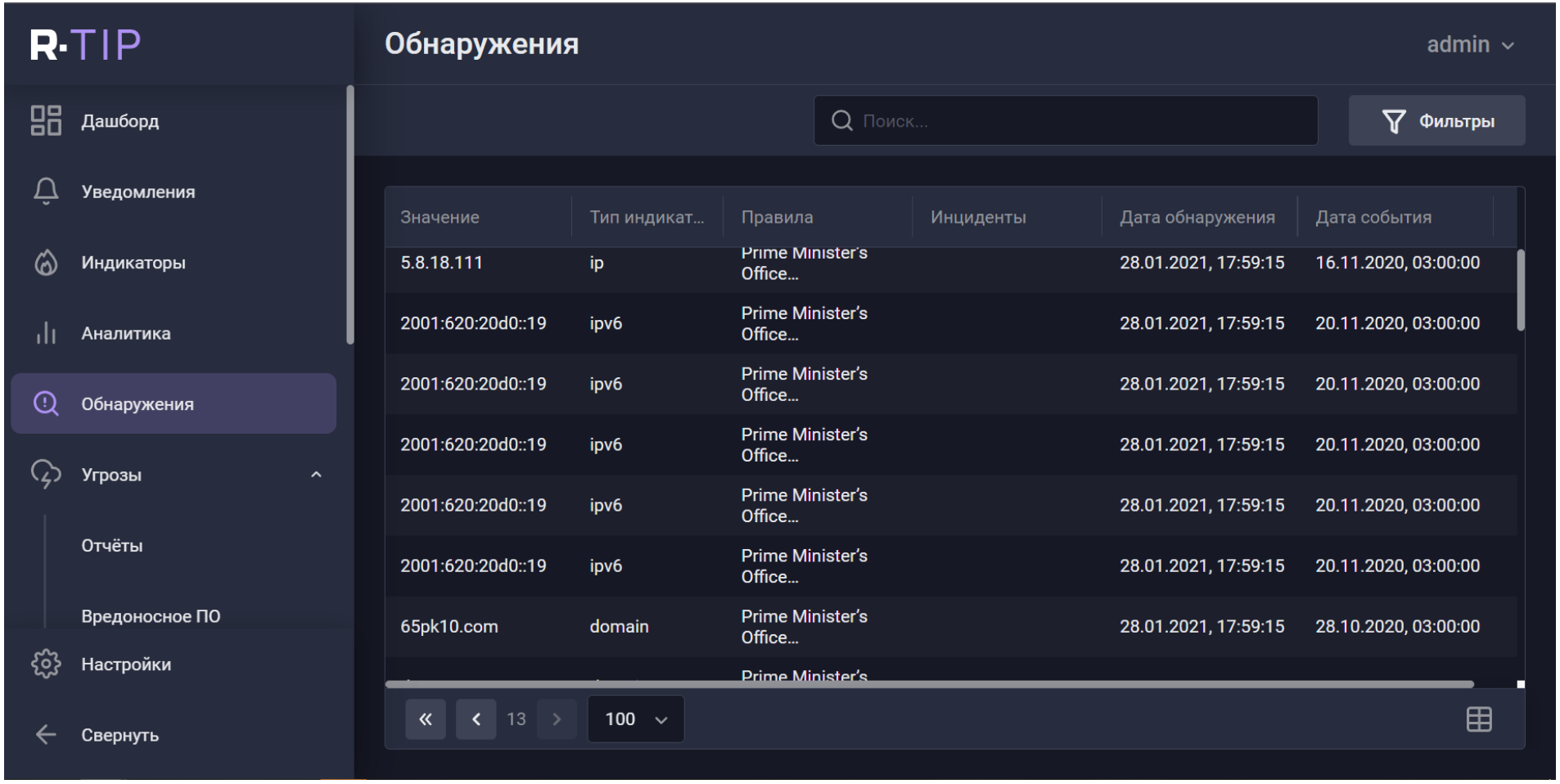
Приоритизация инцидента

Уведомление об инциденте

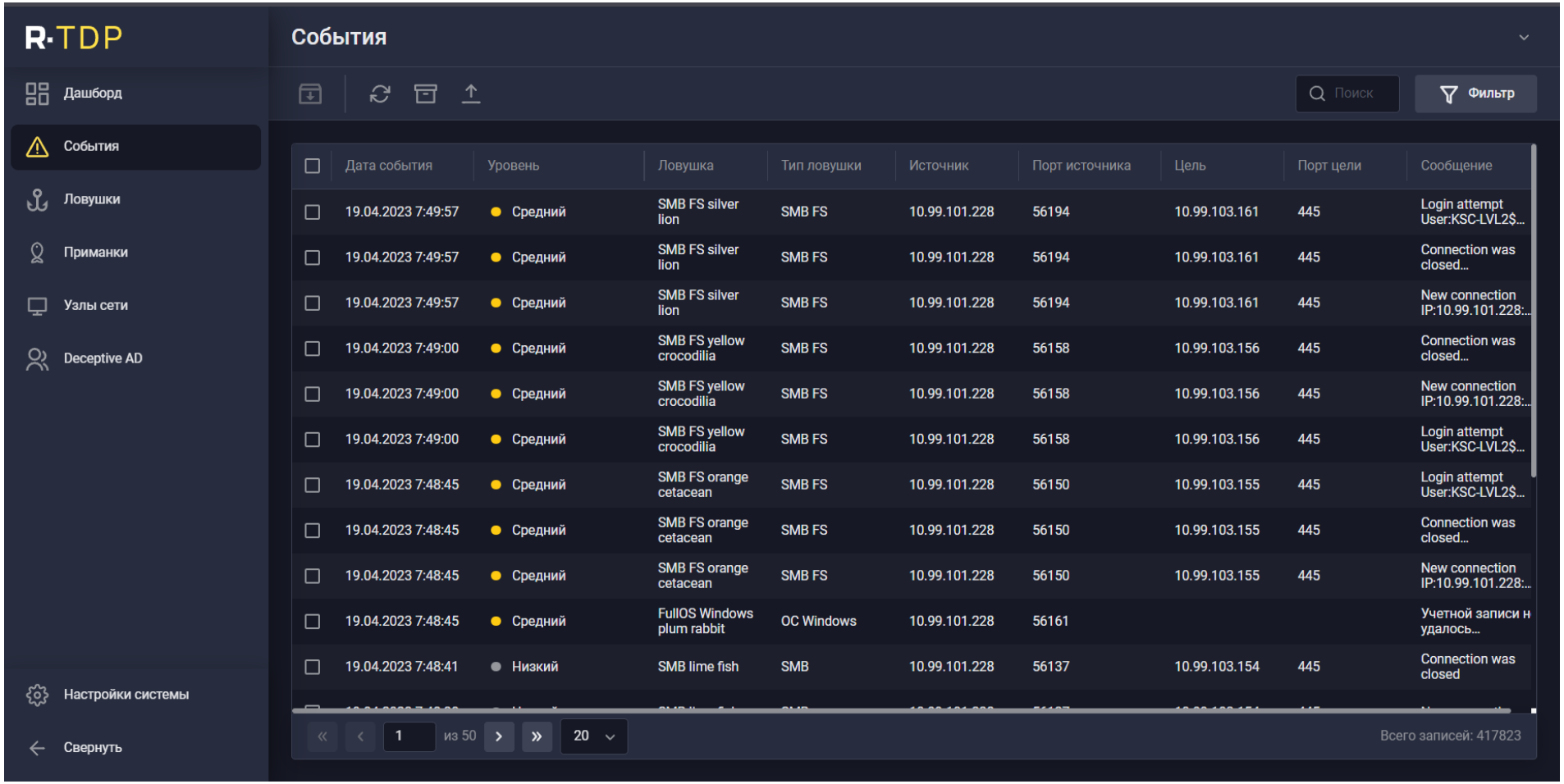
Вектор атаки

- Web
- Email
- Истощение
- Внешние и съемные носители
- Подмена
- Потеря или кража
- Неподходящее использование
- Другое

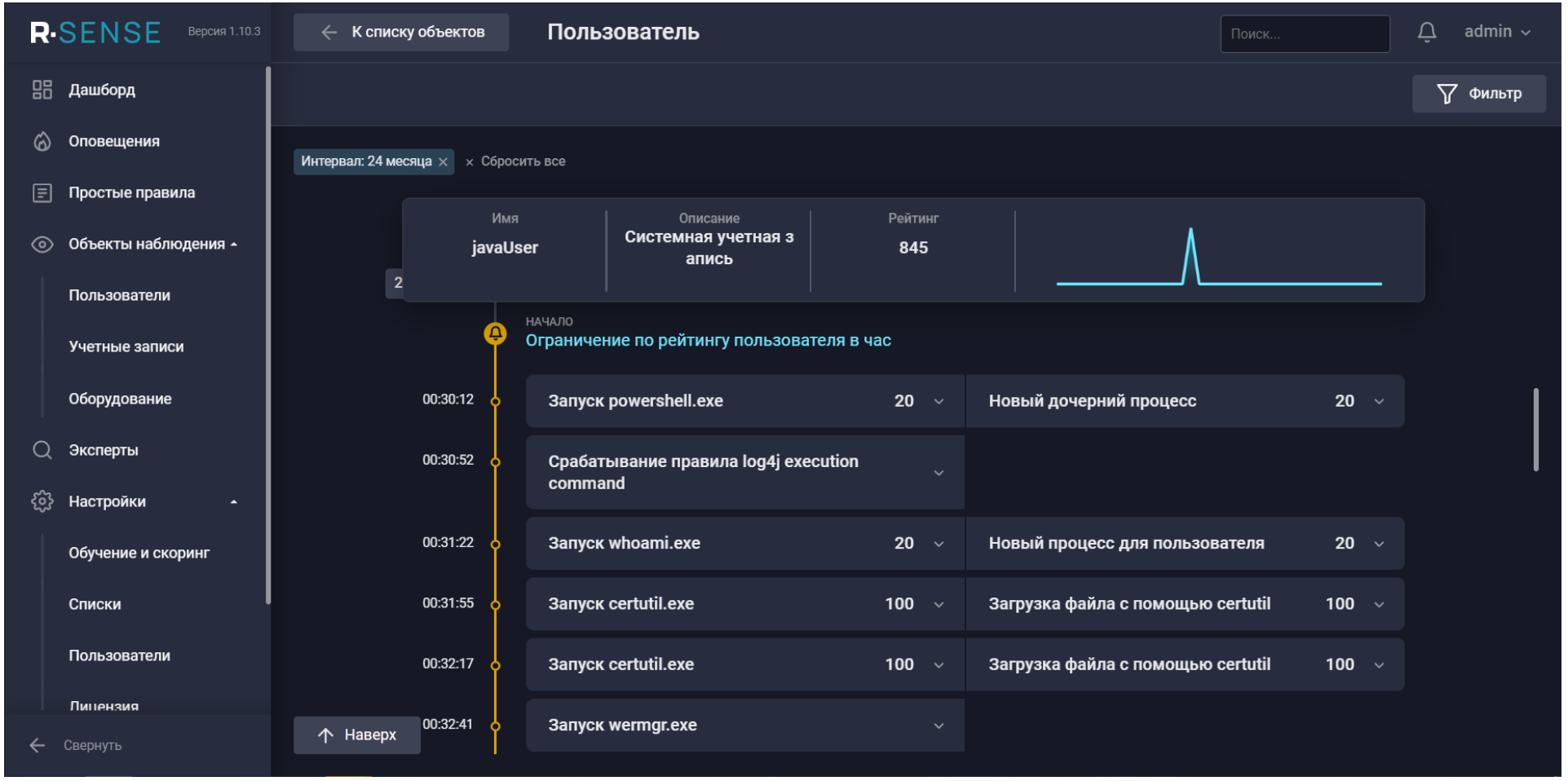
Признаки инцидента



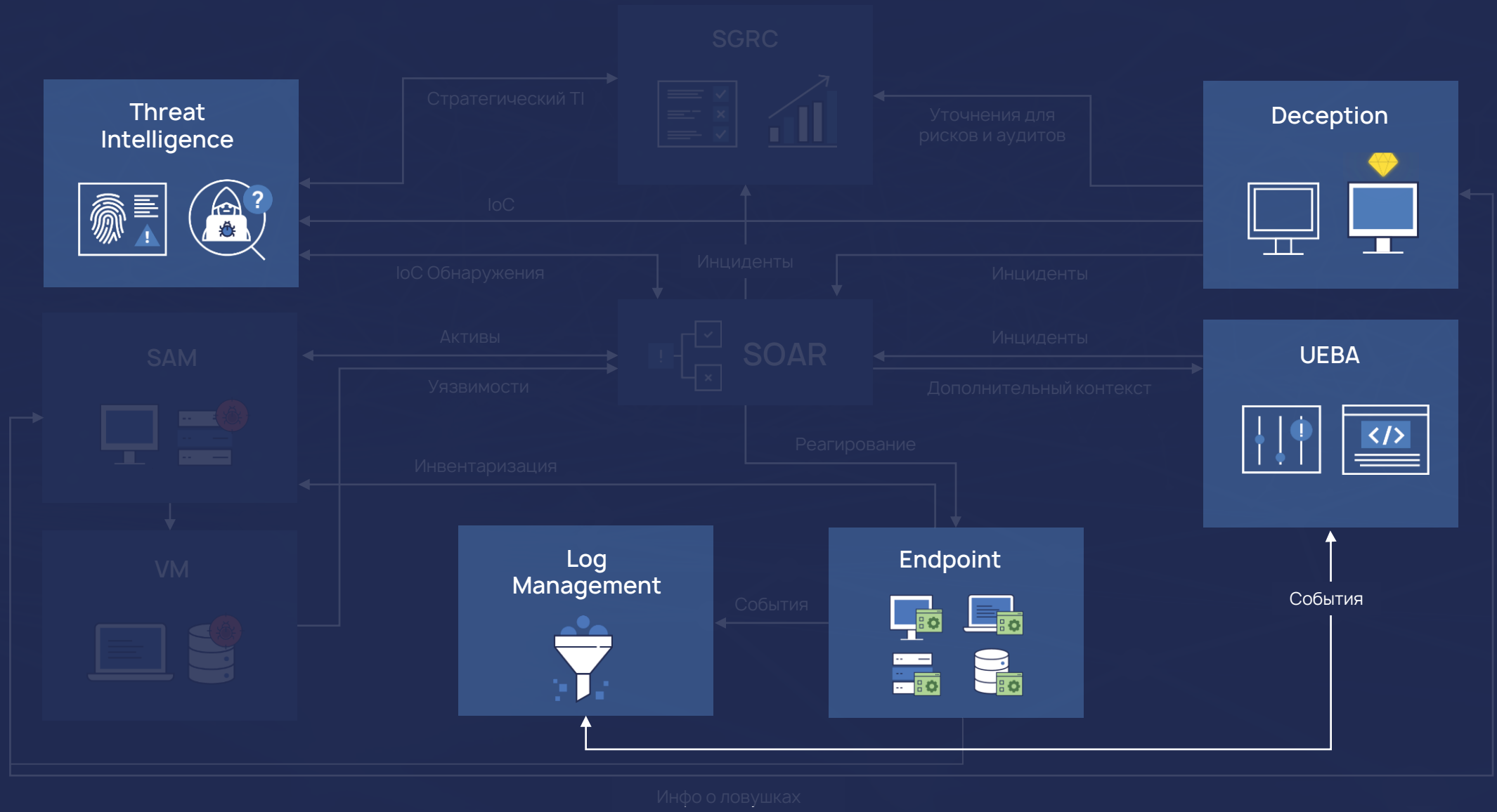
Признаки инцидента



Признаки инцидента

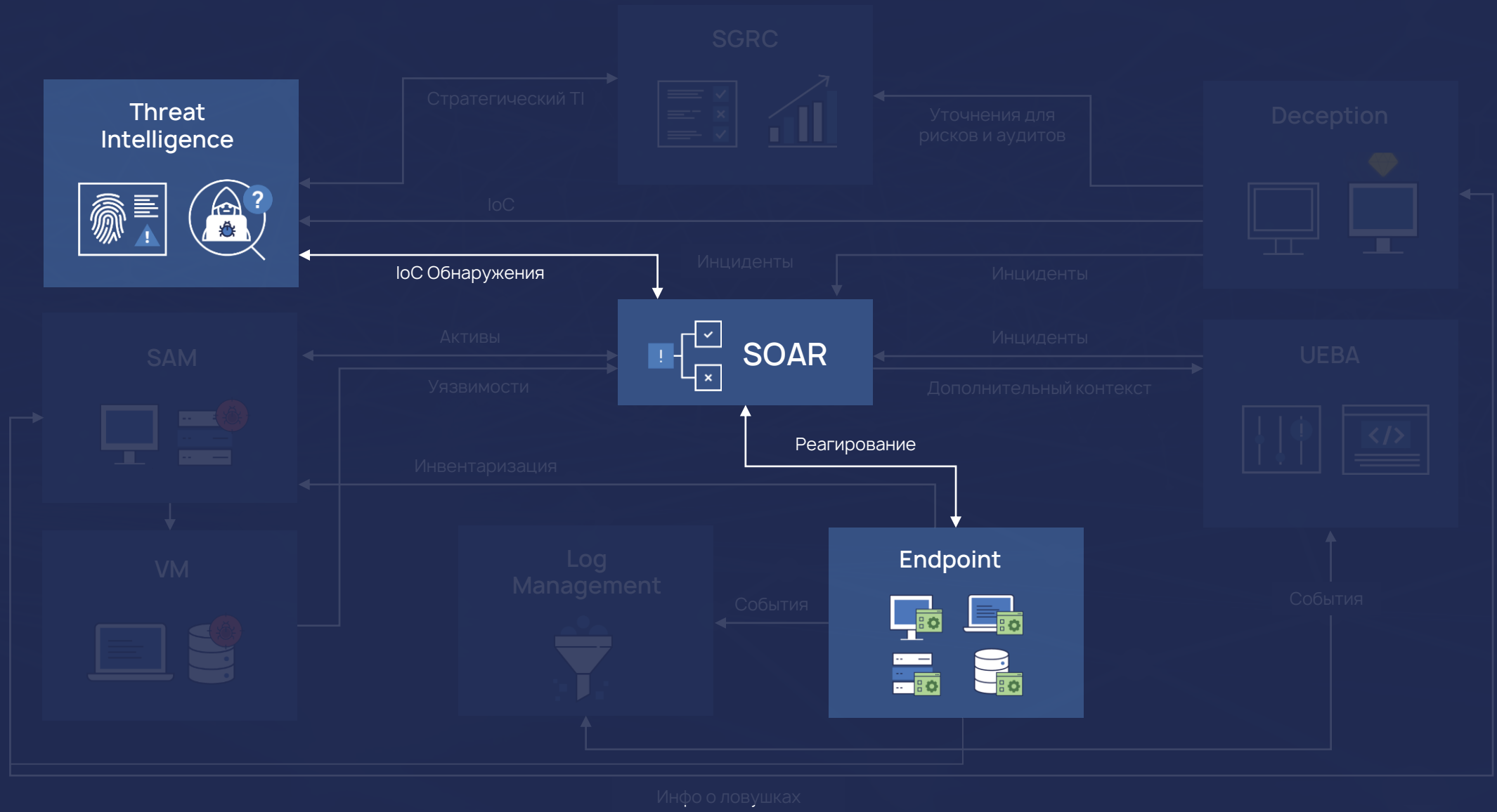


Сбор, анализ и детект



Реагирование

Расследование и реагирование



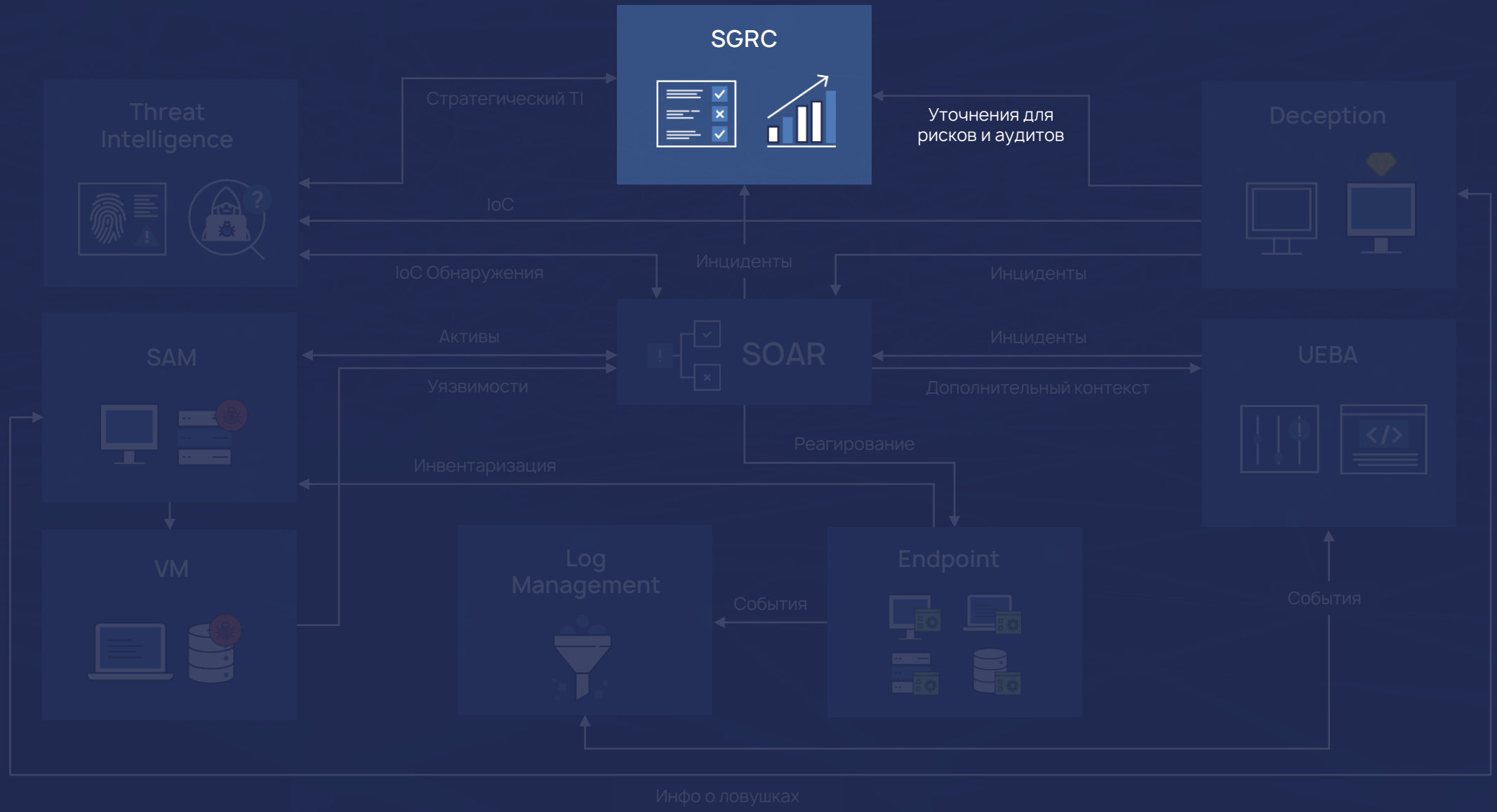
Постинцидентная активность

Что делать потом?

Постинцидентная активность

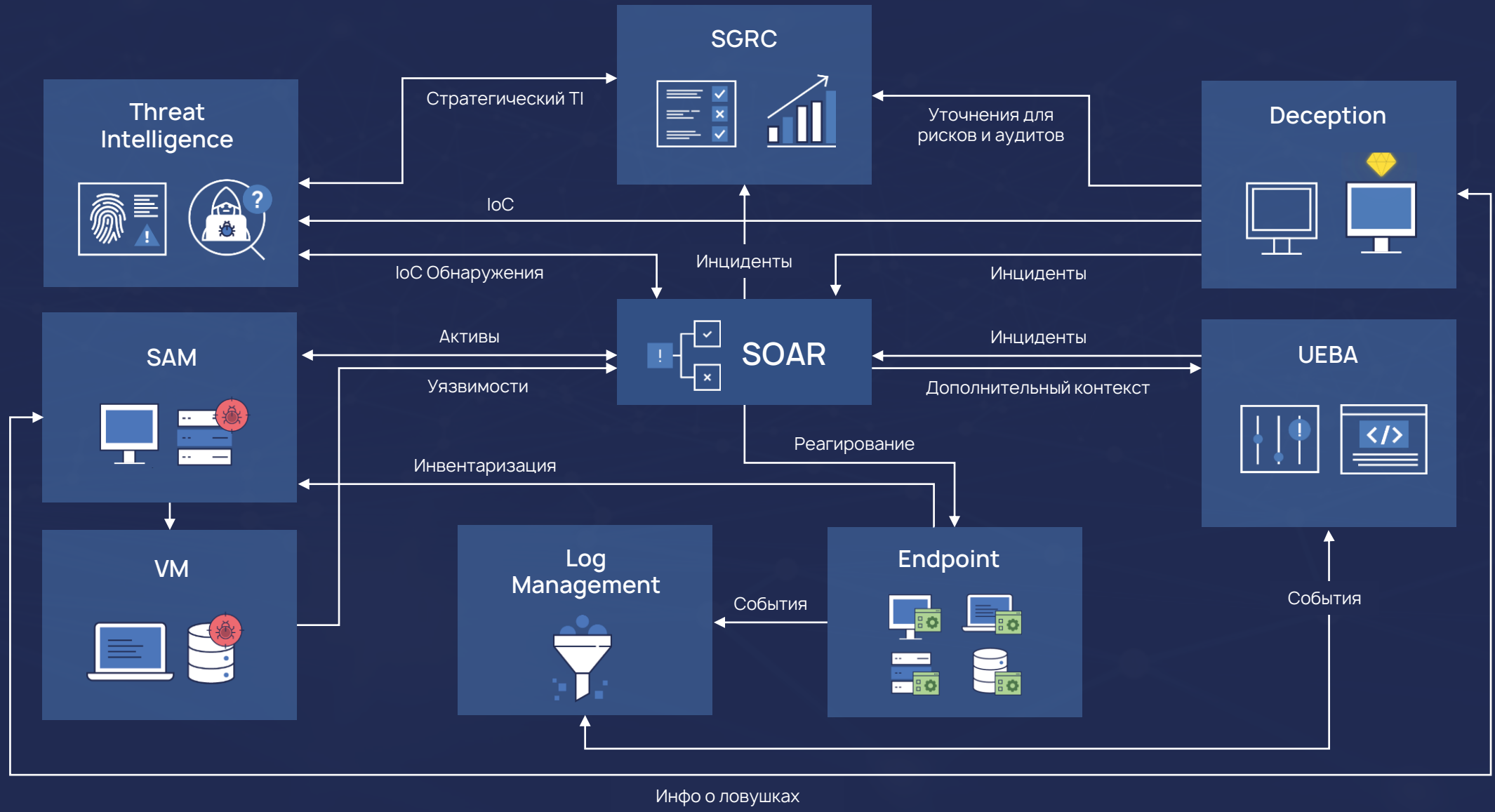
- Какие уроки были вынесены
- Использование данных, собранных об инциденте
- Хранение свидетельств
- Чек-лист по обработке инцидентов

Приведение в соответствие



Итог

Эффективность экосистемы



Спасибо за внимание!