

# R-Vision

## Путь SOC: инциденты и реагирование



**Мельшиян Максим**  
Консультант по ИБ  
[mmelshiyan@rvision.ru](mailto: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?



**ЦОД**



**DC02**

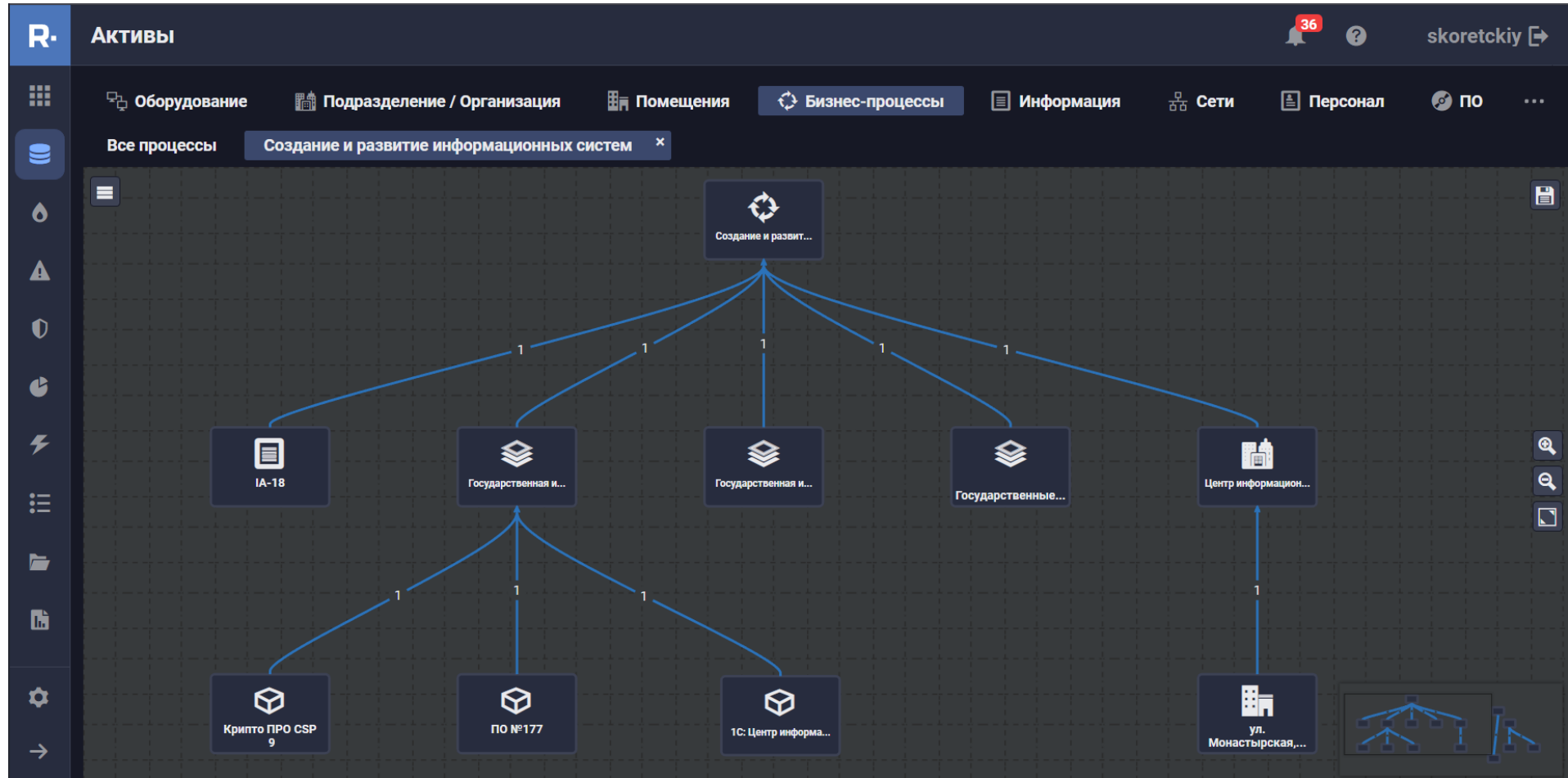


**1С ЗУП:  
Кадровый учет**

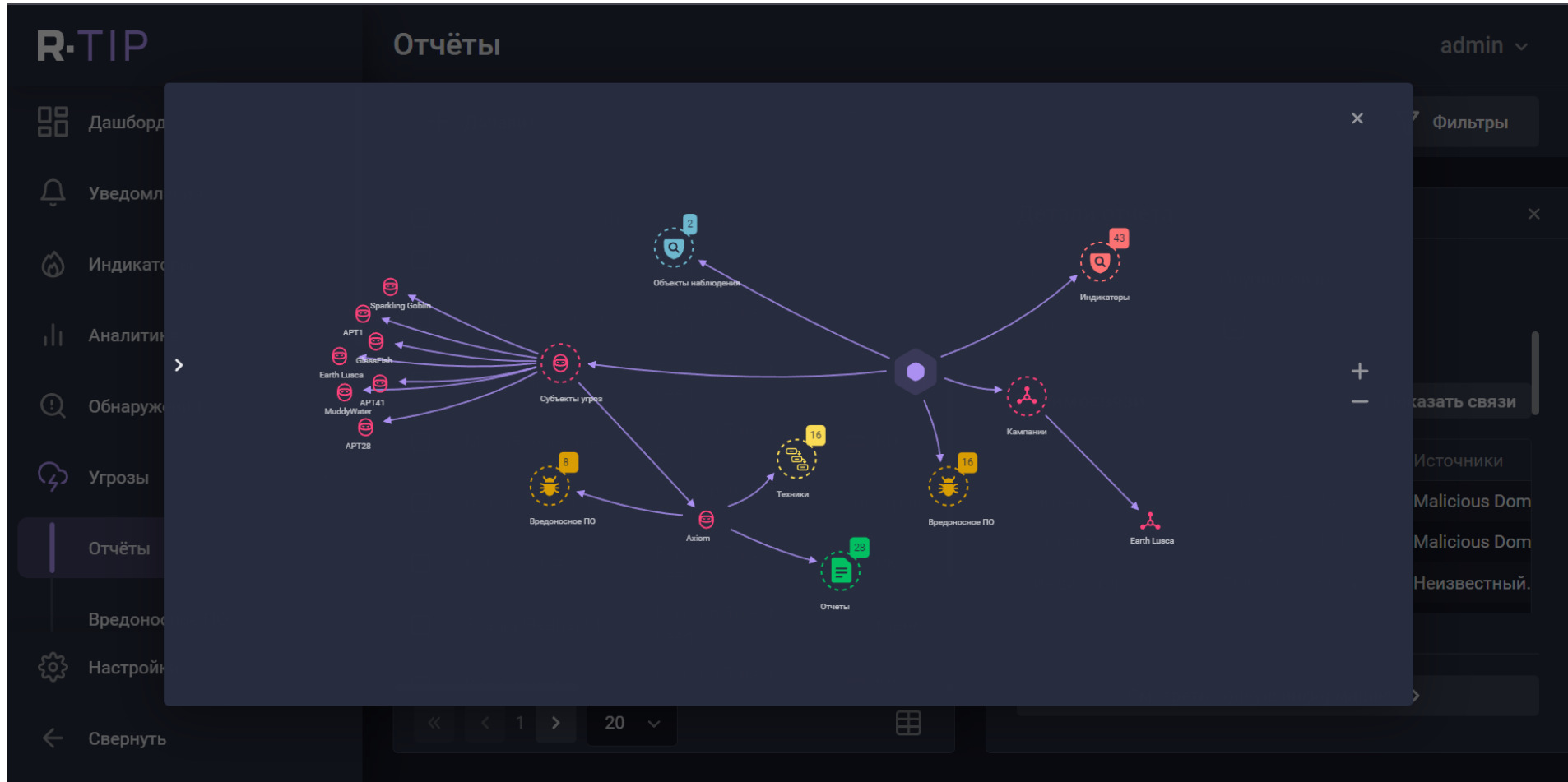


**Сбор данных**

# Что защищаем?



# С кем сражаемся?



# Что может произойти?

The screenshot displays a risk management application interface. The main window is titled "Оценки" (Assessments) and shows a table of risk items. The table has columns for ID, Name, Responsible Person, Status, and Implementation Cost. Two items are visible: RT-135 and RT-136. A detailed view of item RT-135 is shown on the right, including a bar chart comparing current and target values for a specific risk item.

ID	Наименован...	Ответственный	Актив	Стоимость внедрения
RT-135	Внедрение защитной меры: "Регулярное обучение и повышение осведомленнос персонала в области информационнс безопасности"	Дмитрий Салахов (dsalakhov)	IS-13 Автоматизированная ...	400 000
RT-136	Внедрение защитной меры: "Утвержденный регламент мониторинга информационнь системы и систем защиты и реагирования на инциденты"	Захаренко Егор (ezaharenko)	IS-13 Автоматизированная ...	150 000 руб.

**Схема обработки рисков по активу**

Оценка  Качественная  Количественная

IS-13 Автоматизированная банковская система

Автоматизированная банковская система "Учет и проведение кассовых выплат", IA-24

Текущий: 235 105.000  
Целевой: 102 616.000

Снижаемый ущерб: 132 489 000 руб.

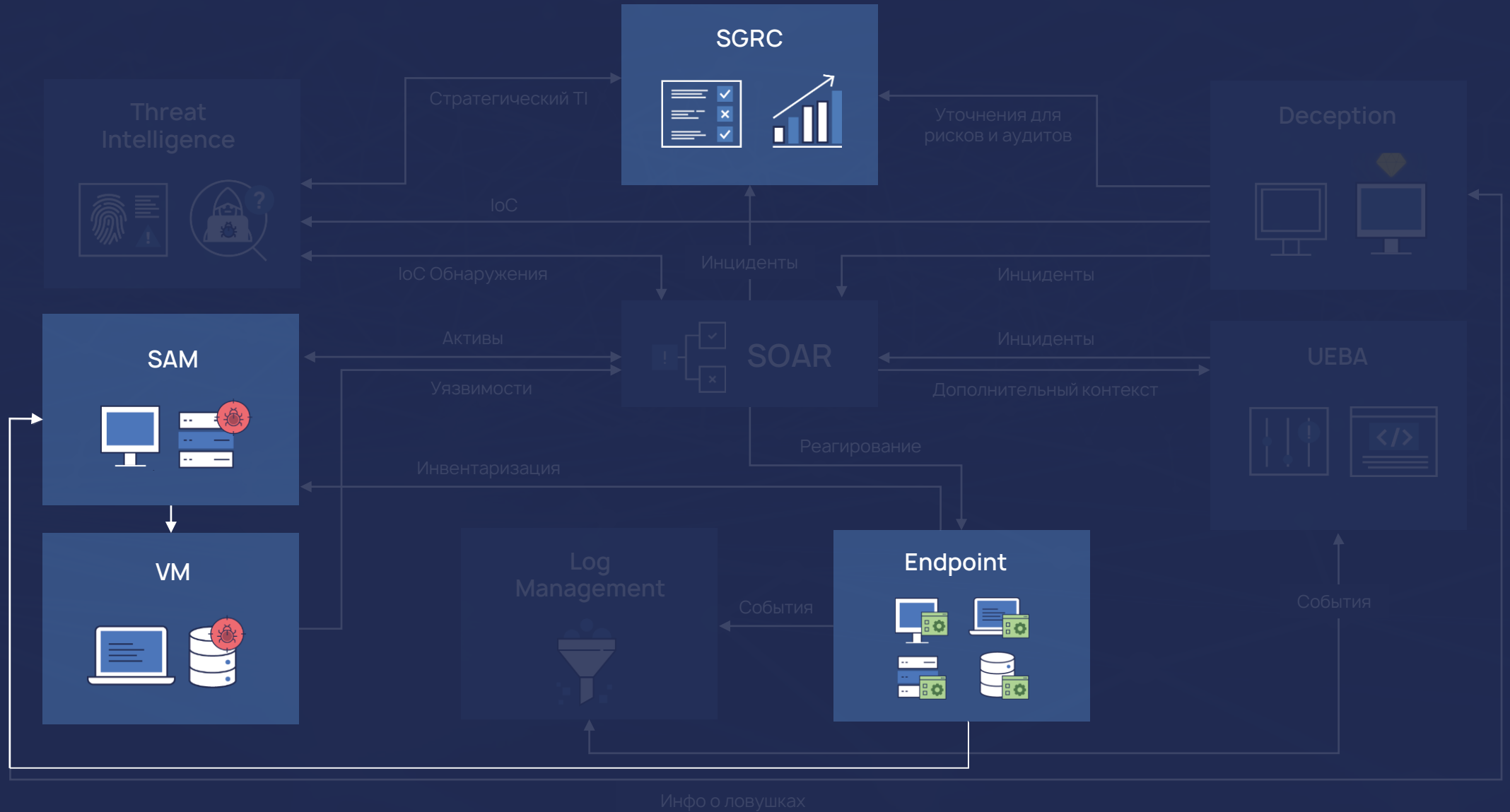
Активы

- Автоматизированная банковская система "Уч...
- Персональные данные посетителей

Бюджет плана 2 050 000 руб.



# 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

The screenshot displays the R-TIP security dashboard. The left sidebar contains navigation options: Дашборд, Уведомления, Индикаторы, Аналитика, **Обнаружения** (highlighted), Угрозы, Отчёты, Вредоносное ПО, Настройки, and Свернуть. The main area is titled 'Обнаружения' and features a search bar and a 'Фильтры' button. Below is a table of detected indicators.

Значение	Тип индикат...	Правила	Инциденты	Дата обнаружения	Дата события
5.8.18.111	ip	Prime Minister's Office...		28.01.2021, 17:59:15	16.11.2020, 03:00:00
2001:620:20d0::19	ipv6	Prime Minister's Office...		28.01.2021, 17:59:15	20.11.2020, 03:00:00
2001:620:20d0::19	ipv6	Prime Minister's Office...		28.01.2021, 17:59:15	20.11.2020, 03:00:00
2001:620:20d0::19	ipv6	Prime Minister's Office...		28.01.2021, 17:59:15	20.11.2020, 03:00:00
2001:620:20d0::19	ipv6	Prime Minister's Office...		28.01.2021, 17:59:15	20.11.2020, 03:00:00
2001:620:20d0::19	ipv6	Prime Minister's Office...		28.01.2021, 17:59:15	20.11.2020, 03:00:00
65pk10.com	domain	Prime Minister's Office...		28.01.2021, 17:59:15	28.10.2020, 03:00:00

At the bottom of the table, there is a pagination control showing '13' items and '100' items per page, along with navigation arrows and a grid icon.

# Признаки инцидента

The screenshot displays the R-TDP interface with a sidebar on the left and a main content area. The sidebar includes navigation options: Дашборд, События (highlighted), Ловушки, Приманки, Узлы сети, Деceptive AD, and Настройки системы. The main content area is titled 'События' and contains a table of event logs. The table has columns for selection, date, level, trap name, trap type, source, source port, target, target port, and message. The events listed are from 19.04.2023 and include various SMB FS and FullOS Windows trap types. The bottom of the interface shows a pagination control (1 из 50) and a total record count (Всего записей: 417823).

<input type="checkbox"/>	Дата события	Уровень	Ловушка	Тип ловушки	Источник	Порт источника	Цель	Порт цели	Сообщение
<input type="checkbox"/>	19.04.2023 7:49:57	Средний	SMB FS silver lion	SMB FS	10.99.101.228	56194	10.99.103.161	445	Login attempt User:KSC-LVL2\$...
<input type="checkbox"/>	19.04.2023 7:49:57	Средний	SMB FS silver lion	SMB FS	10.99.101.228	56194	10.99.103.161	445	Connection was closed...
<input type="checkbox"/>	19.04.2023 7:49:57	Средний	SMB FS silver lion	SMB FS	10.99.101.228	56194	10.99.103.161	445	New connection IP:10.99.101.228:...
<input type="checkbox"/>	19.04.2023 7:49:00	Средний	SMB FS yellow crocodilia	SMB FS	10.99.101.228	56158	10.99.103.156	445	Connection was closed...
<input type="checkbox"/>	19.04.2023 7:49:00	Средний	SMB FS yellow crocodilia	SMB FS	10.99.101.228	56158	10.99.103.156	445	New connection IP:10.99.101.228:...
<input type="checkbox"/>	19.04.2023 7:49:00	Средний	SMB FS yellow crocodilia	SMB FS	10.99.101.228	56158	10.99.103.156	445	Login attempt User:KSC-LVL2\$...
<input type="checkbox"/>	19.04.2023 7:48:45	Средний	SMB FS orange cetacean	SMB FS	10.99.101.228	56150	10.99.103.155	445	Login attempt User:KSC-LVL2\$...
<input type="checkbox"/>	19.04.2023 7:48:45	Средний	SMB FS orange cetacean	SMB FS	10.99.101.228	56150	10.99.103.155	445	Connection was closed...
<input type="checkbox"/>	19.04.2023 7:48:45	Средний	SMB FS orange cetacean	SMB FS	10.99.101.228	56150	10.99.103.155	445	New connection IP:10.99.101.228:...
<input type="checkbox"/>	19.04.2023 7:48:45	Средний	FullOS Windows plum rabbit	OC Windows	10.99.101.228	56161			Учетной записи не удалось...
<input type="checkbox"/>	19.04.2023 7:48:41	Низкий	SMB lime fish	SMB	10.99.101.228	56137	10.99.103.154	445	Connection was closed

# Признаки инцидента

**R-SENSE** Версия 1.10.3

← К списку объектов **Пользователь** Поиск... admin

Фильтр

Интервал: 24 месяца × Сбросить все

Имя	Описание	Рейтинг	
javaUser	Системная учетная запись	845	

2

НАЧАЛО

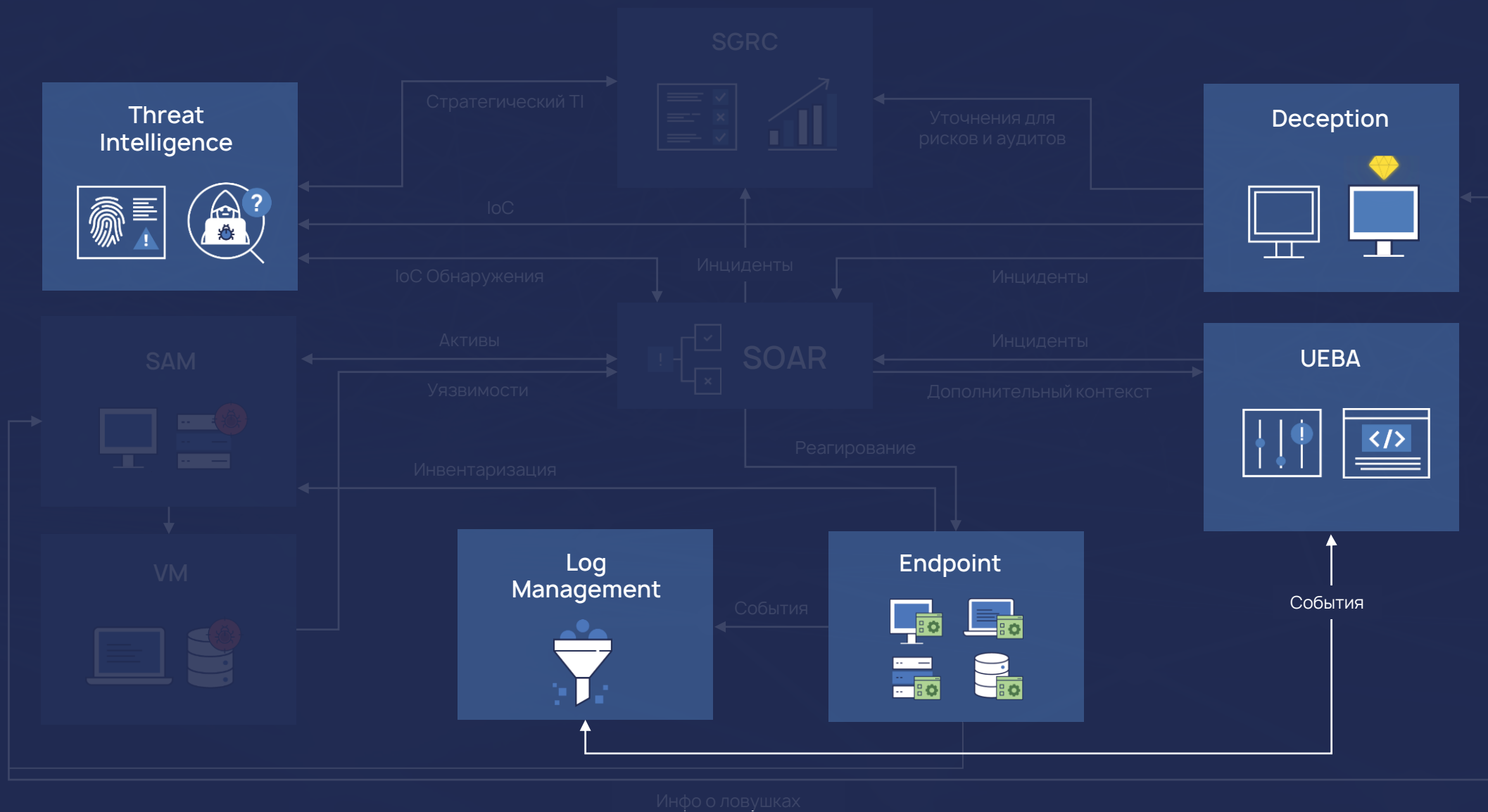
Ограничение по рейтингу пользователя в час

00:30:12	Запуск powershell.exe	20	Новый дочерний процесс	20
00:30:52	Срабатывание правила log4j execution command			
00:31:22	Запуск whoami.exe	20	Новый процесс для пользователя	20
00:31:55	Запуск certutil.exe	100	Загрузка файла с помощью certutil	100
00:32:17	Запуск certutil.exe	100	Загрузка файла с помощью certutil	100
00:32:41	Запуск wermgr.exe			

← Свернуть

↑ Наверх

# Сбор, анализ и детект

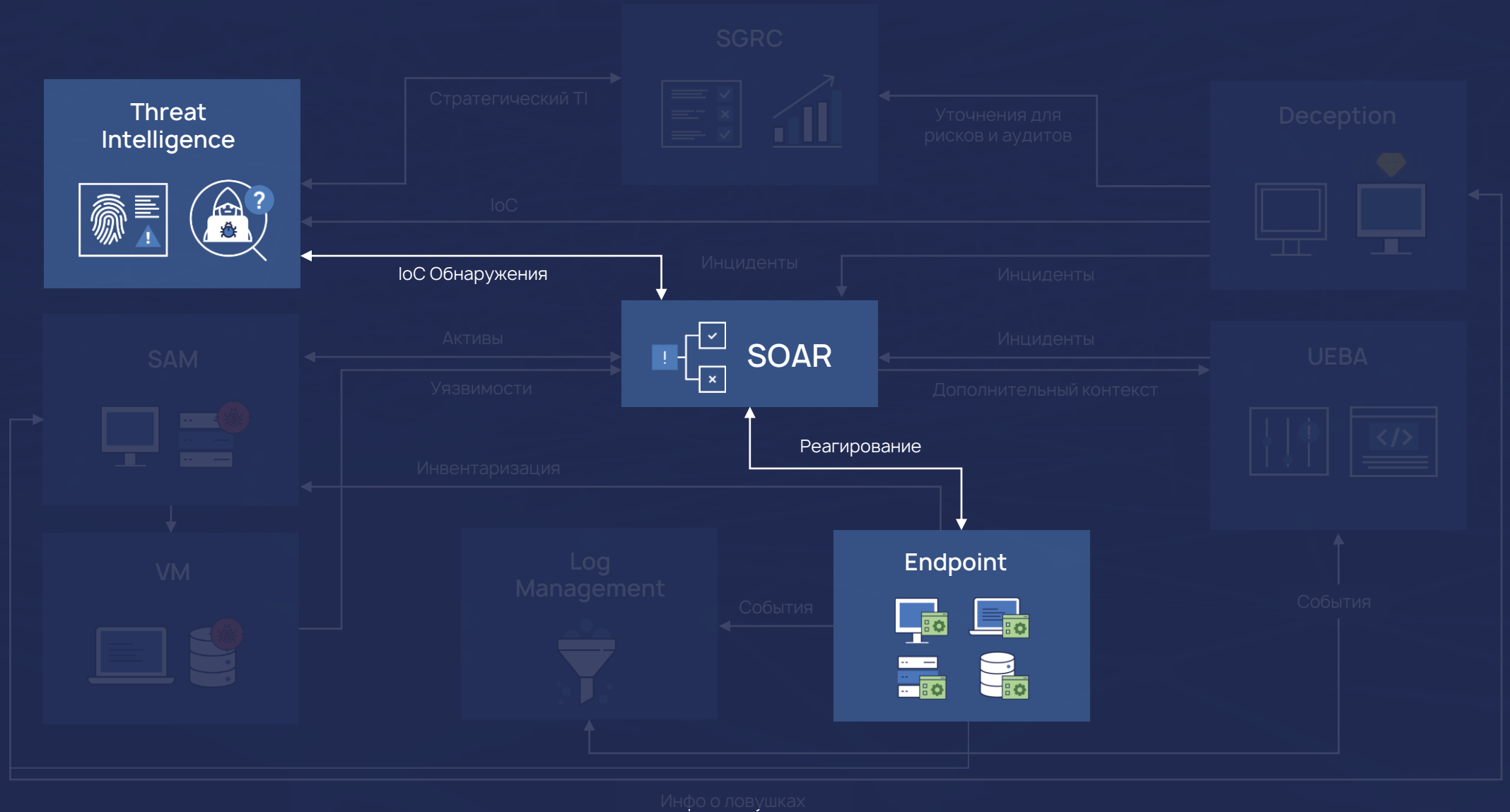




# Реагирование



# Расследование и реагирование





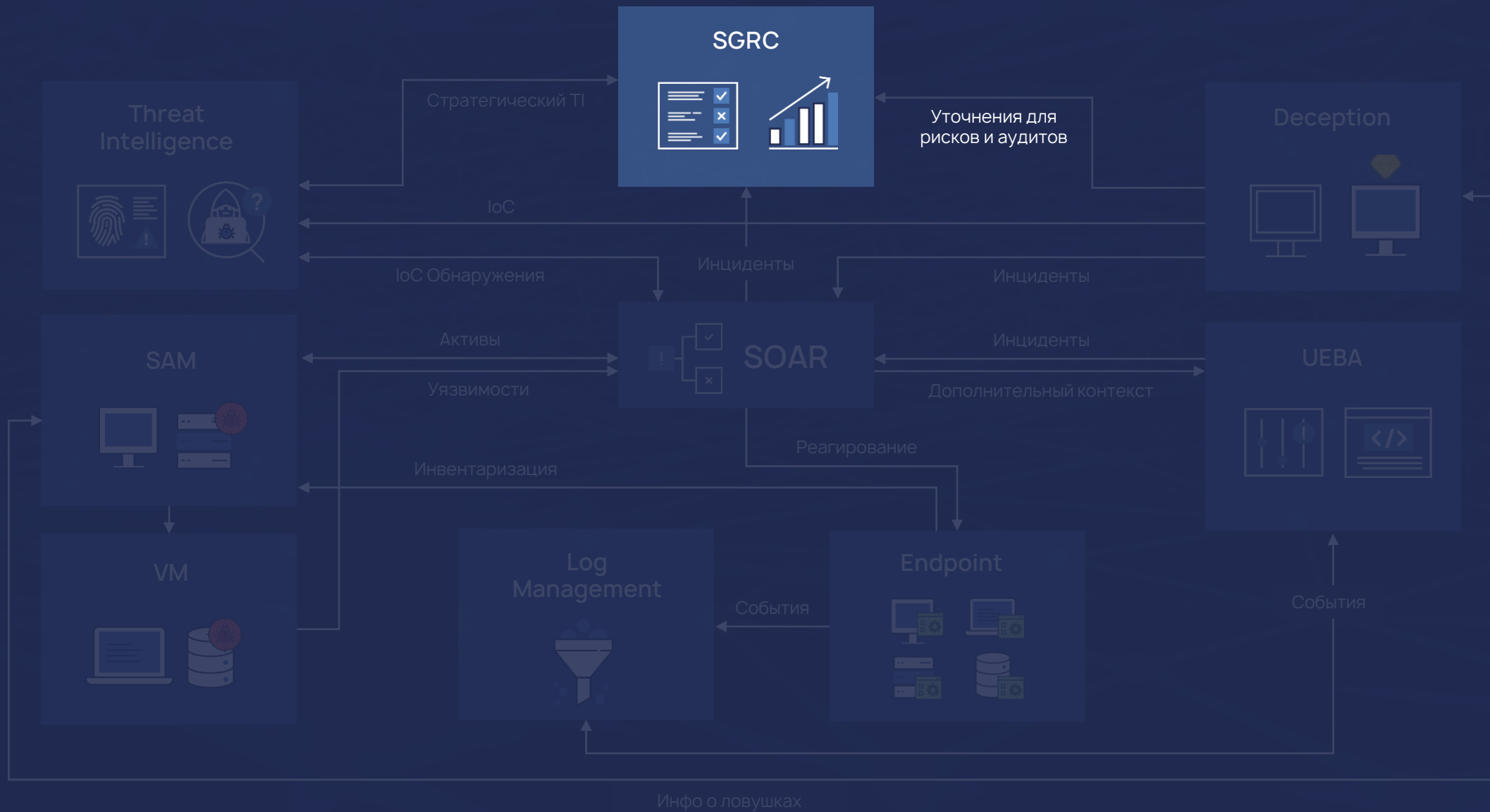
# Постинцидентная активность

Что делать потом?

# Постинцидентная активность

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

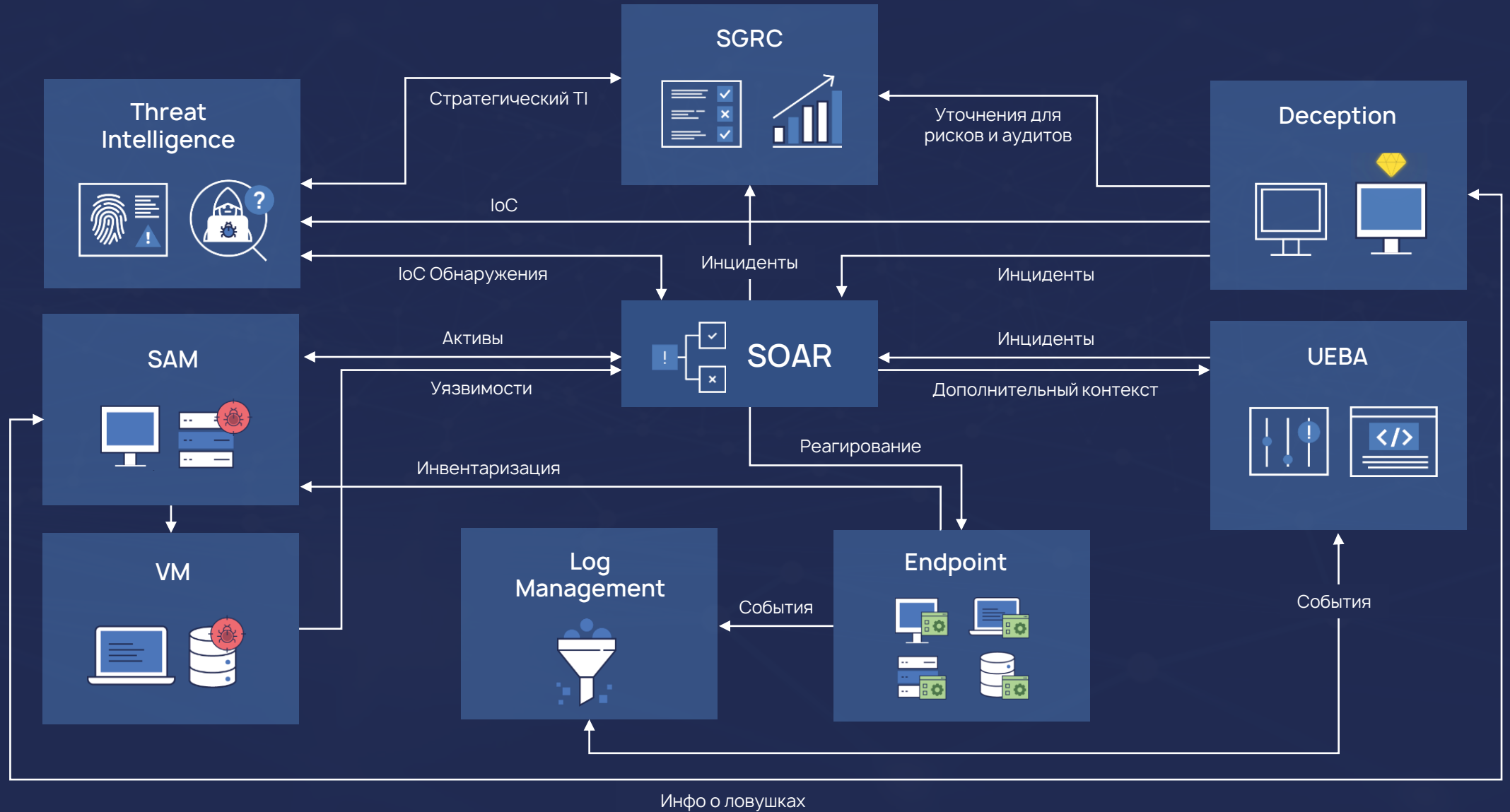
# Приведение в соответствие





**ИТОГ**

# Эффективность экосистемы





**Спасибо за внимание!**