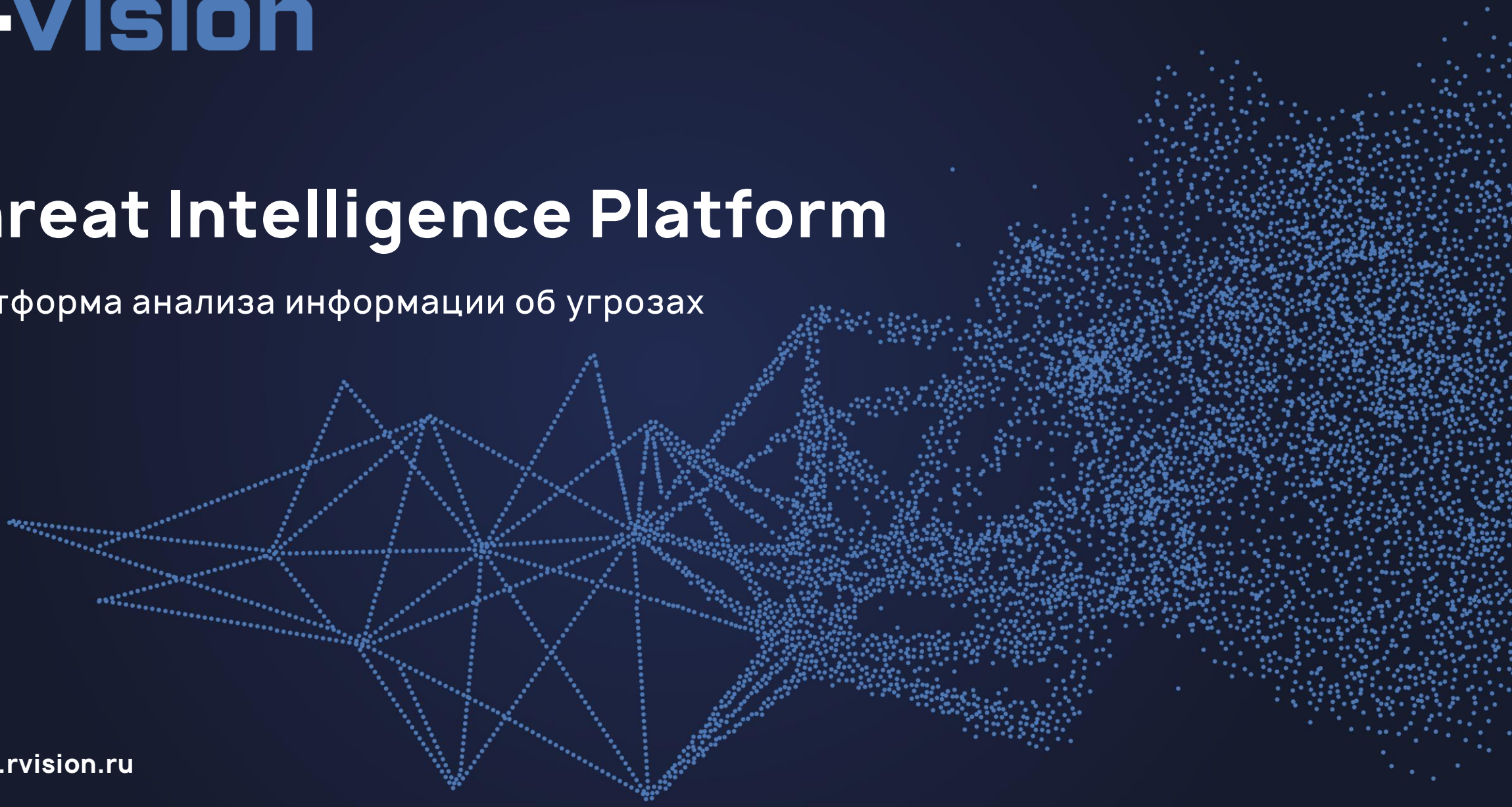
R·Vision

# Threat Intelligence Platform

Платформа анализа информации об угрозах



www.rvision.ru

# Что такое Threat Intelligence?

**Threat intelligence – это знания об угрозах, полученные в результате анализа и интерпретации данных**

**Операционный уровень**

**Индикаторы компрометации (IP адреса, домены, хэши, C&C адреса ботнетов и т.д.)**

↓

**Выявление и блокировка скрытых угроз, реагирование**

**Тактический уровень**

**Тактика, техники и процедуры (TTPs) злоумышленников**

↓

**Прогнозирование атак, защитные меры, обнаружение**

**Стратегический уровень**

**Отчеты об угрозах**

↓

**Принятие стратегических решений в области ИБ**

# Использование Threat Intelligence

## Кто: Люди

CISO

Риск-менеджер

Аналитик SOC

TI аналитик

## Для чего: Процессы

Реагирование на инциденты

Управление уязвимостями

Мошенничество

Риски

Операционная безопасность

Метрики ИБ

## Как: Технологии

Firewall


EDR


IPS

UEBA

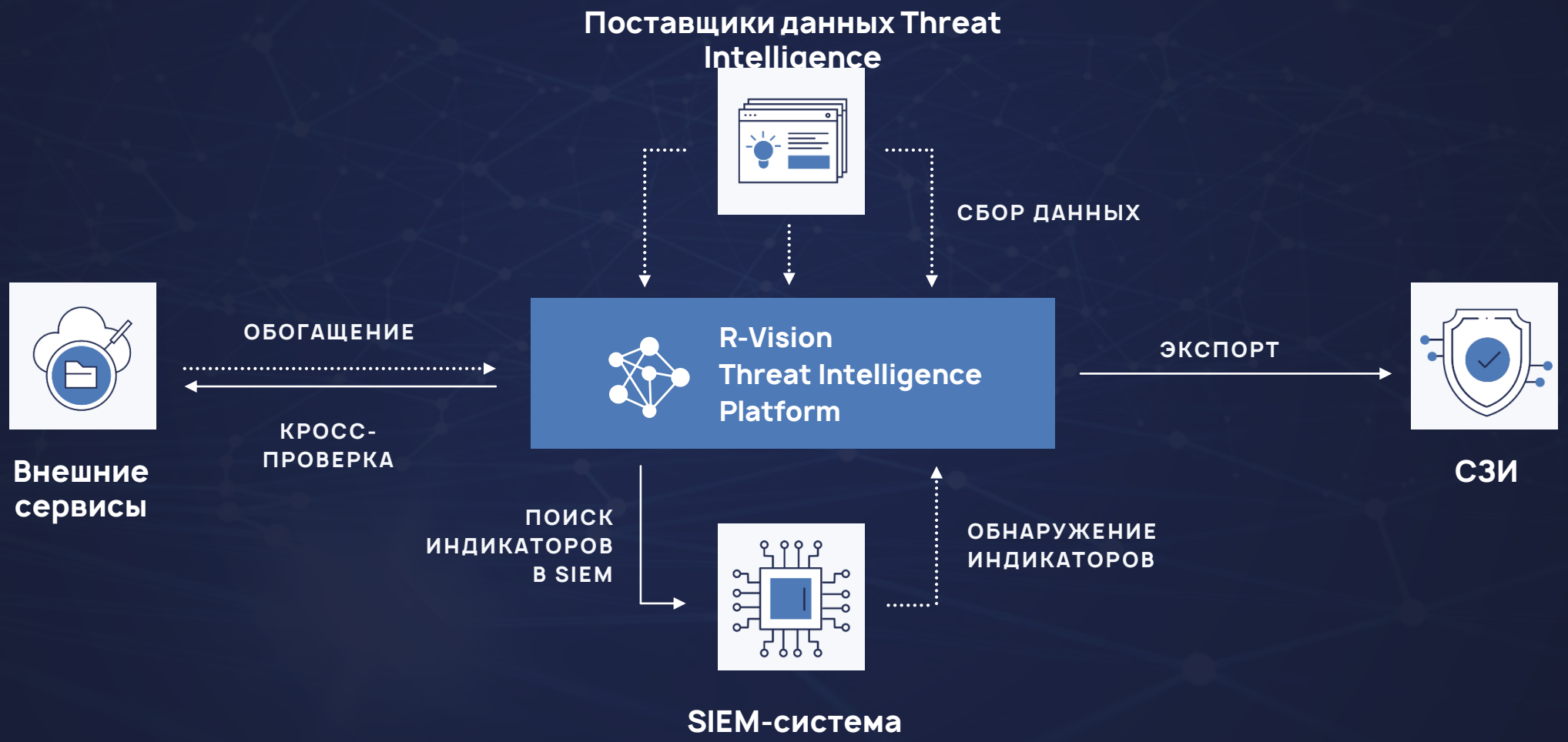
Безопасность облаков

TI платформы



Согласно Gartner, 2019

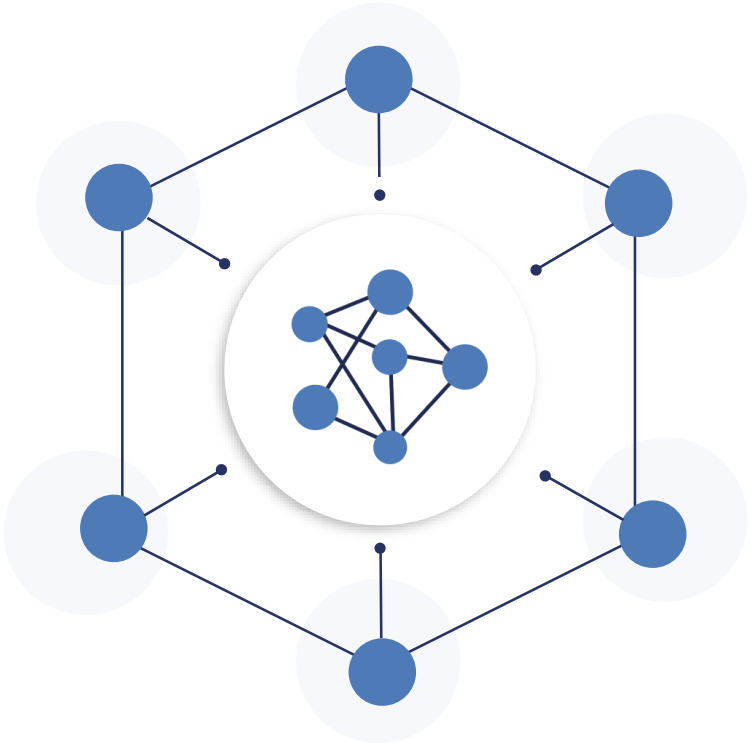
# Схема работы R-Vision TIP



# Возможности R-Vision TIP

**Сбор**
индикаторов из разных источников

**Автоматизация**
повторяющихся операций
и сценариев использования
индикаторов



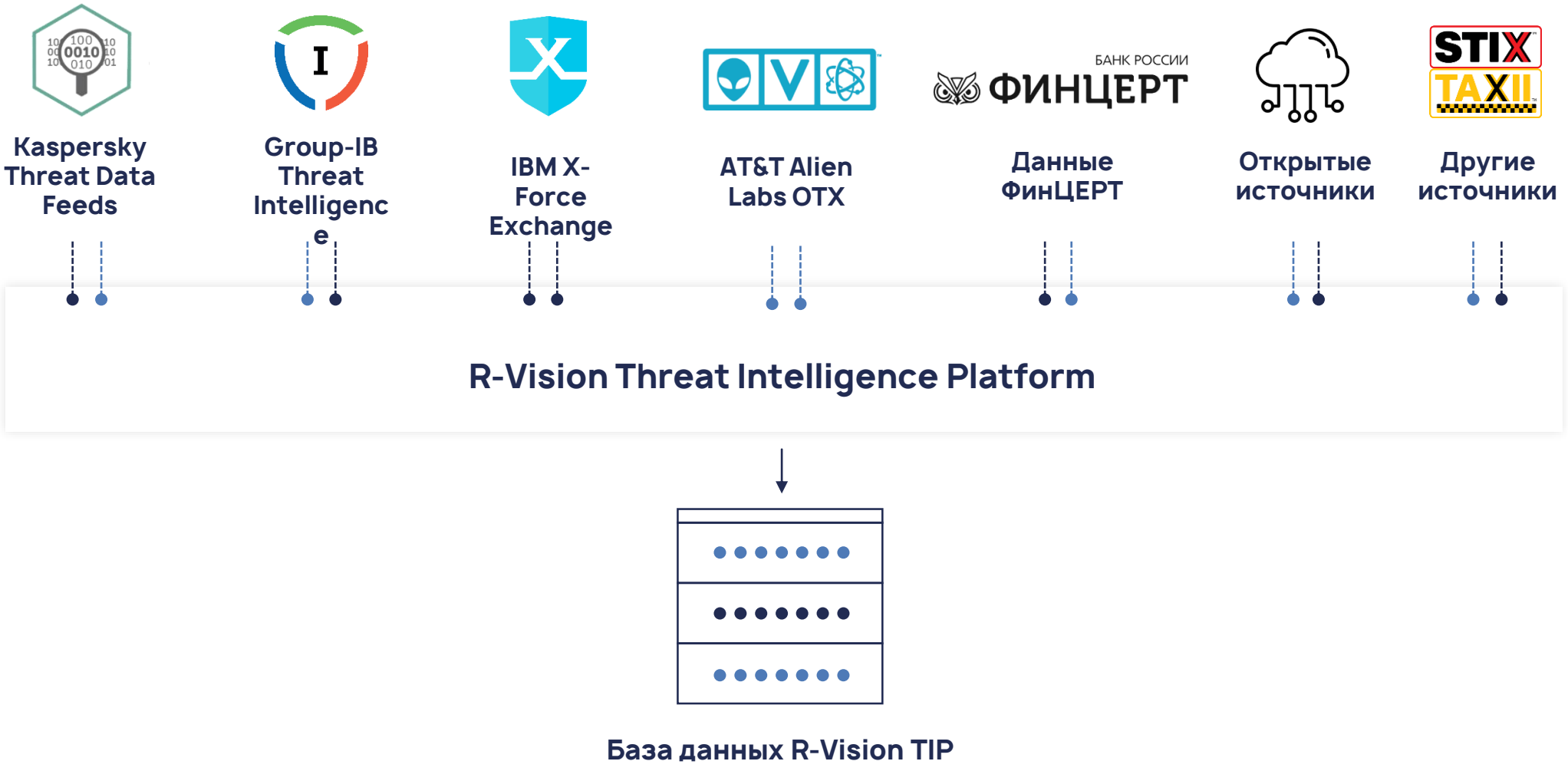
**Обработка и обогащение**
данных информацией
из внешних систем,
нормализация

**Экспорт**
на средства защиты для
мониторинга и блокировки

**Анализ взаимосвязей**
индикаторов между собой, с
отчетами, уязвимостями,
вредоносным ПО

**Обнаружение**
индикаторов компрометации внутри инфраструктуры
и оповещение

# Поставщики Threat Intelligence



# Обработка и обогащение данных

**Обработка = преобразование в пригодную для дальнейшего использования форму**

**Нормализация**

**Дедупликация**

**Приведение к единому структурированному формату**

**Обогащение контекстом с помощью внешних сервисов:**

- VirusTotal
- Hybrid Analysis
- OPSWAT Metadefender
- Shodan
- RiskIQ
- MaxMind
- Sypex
- Ipgeolocation.io
- Whois
- ThreatCrowd
- TotalHash
- другие

# Анализ взаимосвязей

**Формирование целостной картины угрозы для правильной интерпретации данных аналитиком.**

**Анализ связанных с индикатором данных:**

Отчеты о технике, тактике и процедурах (TTPs) злоумышленника

Уязвимости (CVE), список уязвимого ПО (CPE), дефекты безопасности (CWE) из баз NVD (NIST) и MITRE


Вредоносное ПО

Другие связанные индикаторы

**Предусмотрено создание и изменение собственных индикаторов**

# Конструктор бюллетеней

**Создание собственных информационных материалов для повышения осведомленности различных кругов заинтересованных лиц**

**Формирование бюллетеней двух типов: по угрозам и по уязвимостям**

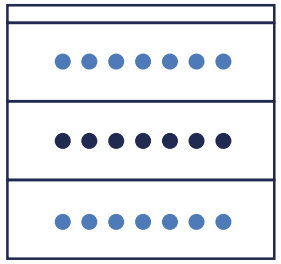
**Автозаполнение данных**

**Добавление в бюллетень дополнительных свидетельств (изображения, аннотации)**

**Рассылка бюллетеней по подведомственным структурам**

**Экспорт бюллетеней на внешние системы с помощью API**

# Интеграция с используемыми СЗИ



**Автоматическая выгрузка индикаторов на СЗИ для немедленной блокировки**

paloalto NETWORKS

CISCO

FORTINET

Check Point SOFTWARE TECHNOLOGIES LTD

**Другие**

# Мониторинг индикаторов

**Ретроспективный и реал-тайм поиск релевантных индикаторов в событиях SIEM**

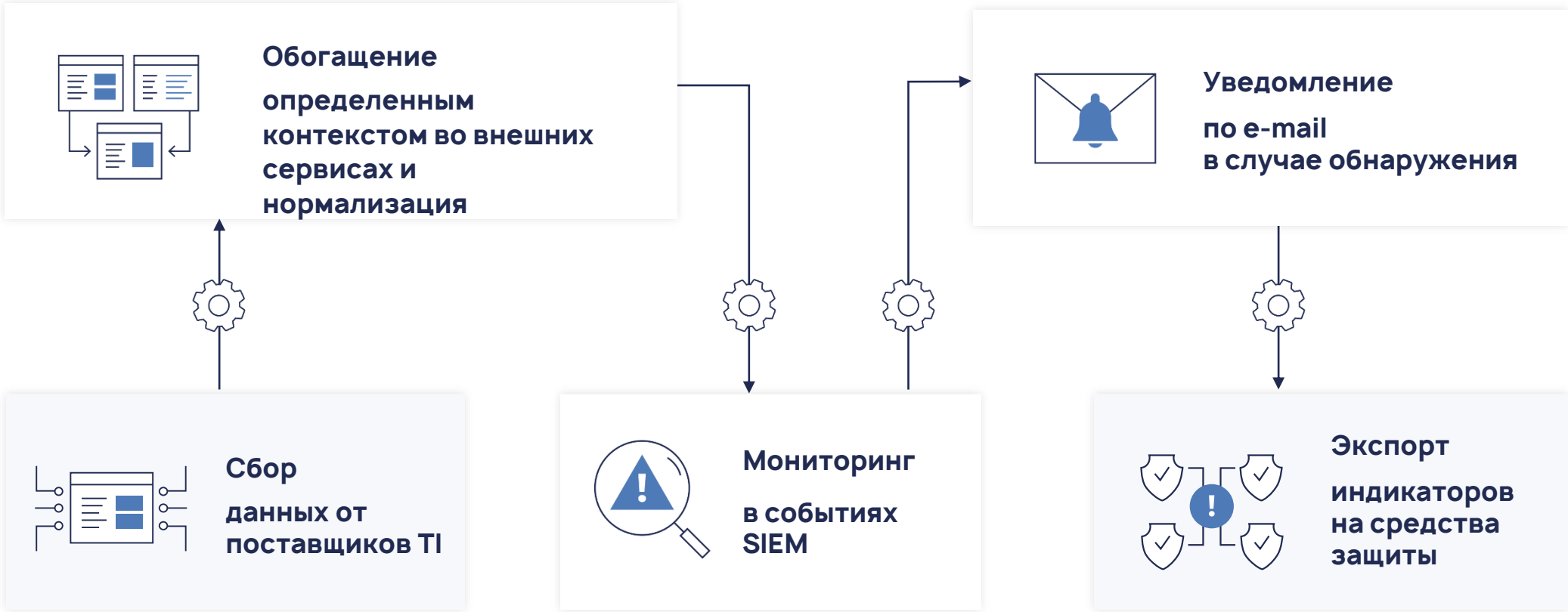

- QRadar
- ArcSight
- MaxPatrol SIEM
- Другие SIEM

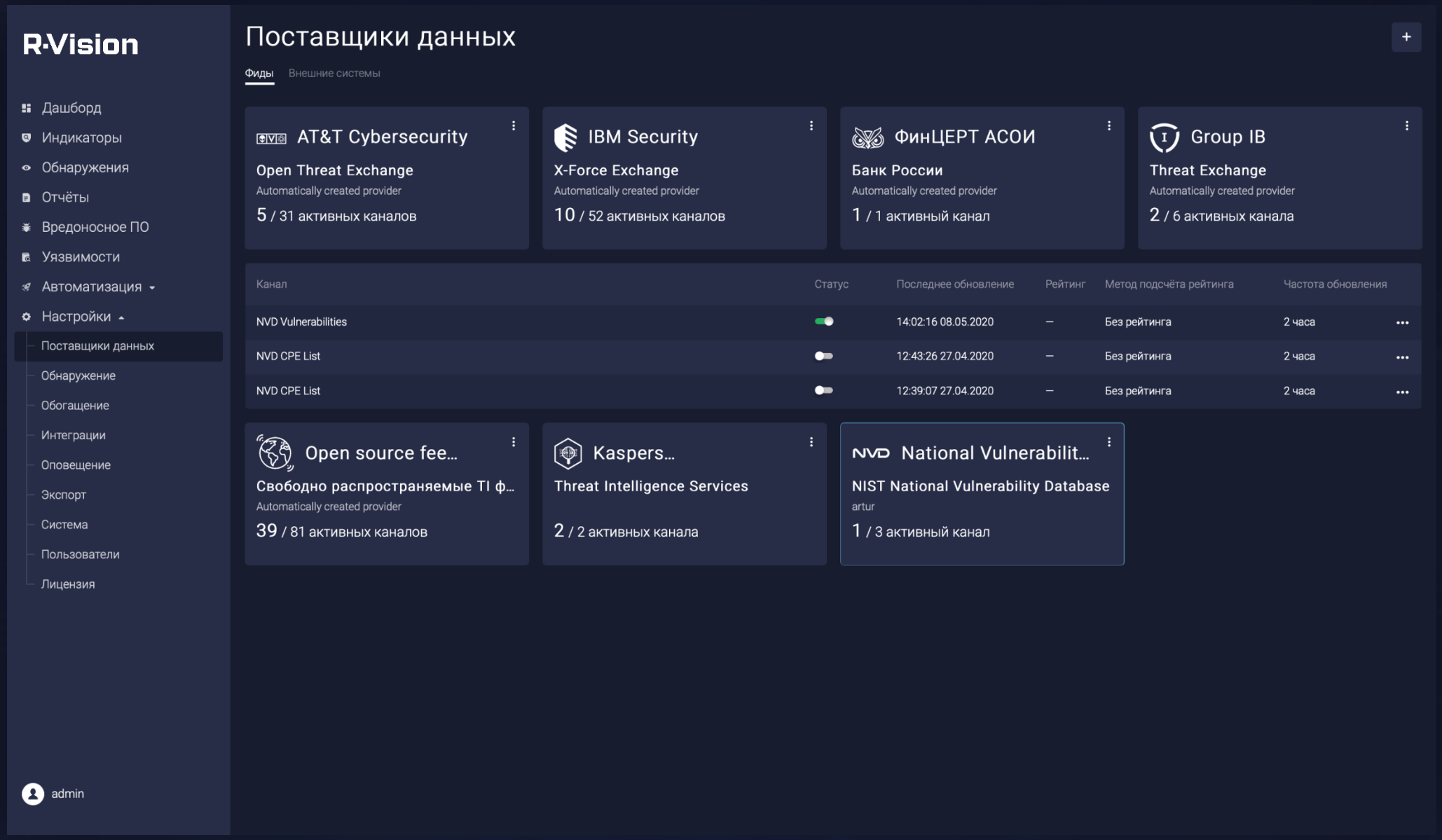
# Распределенная инсталляция сенсоров SIEM


**Возможность распределенной установки сенсоров интеграции с SIEM-системами для сбора индикаторов компрометации ближе к потокам данных**

# Автоматизация работы с индикаторами

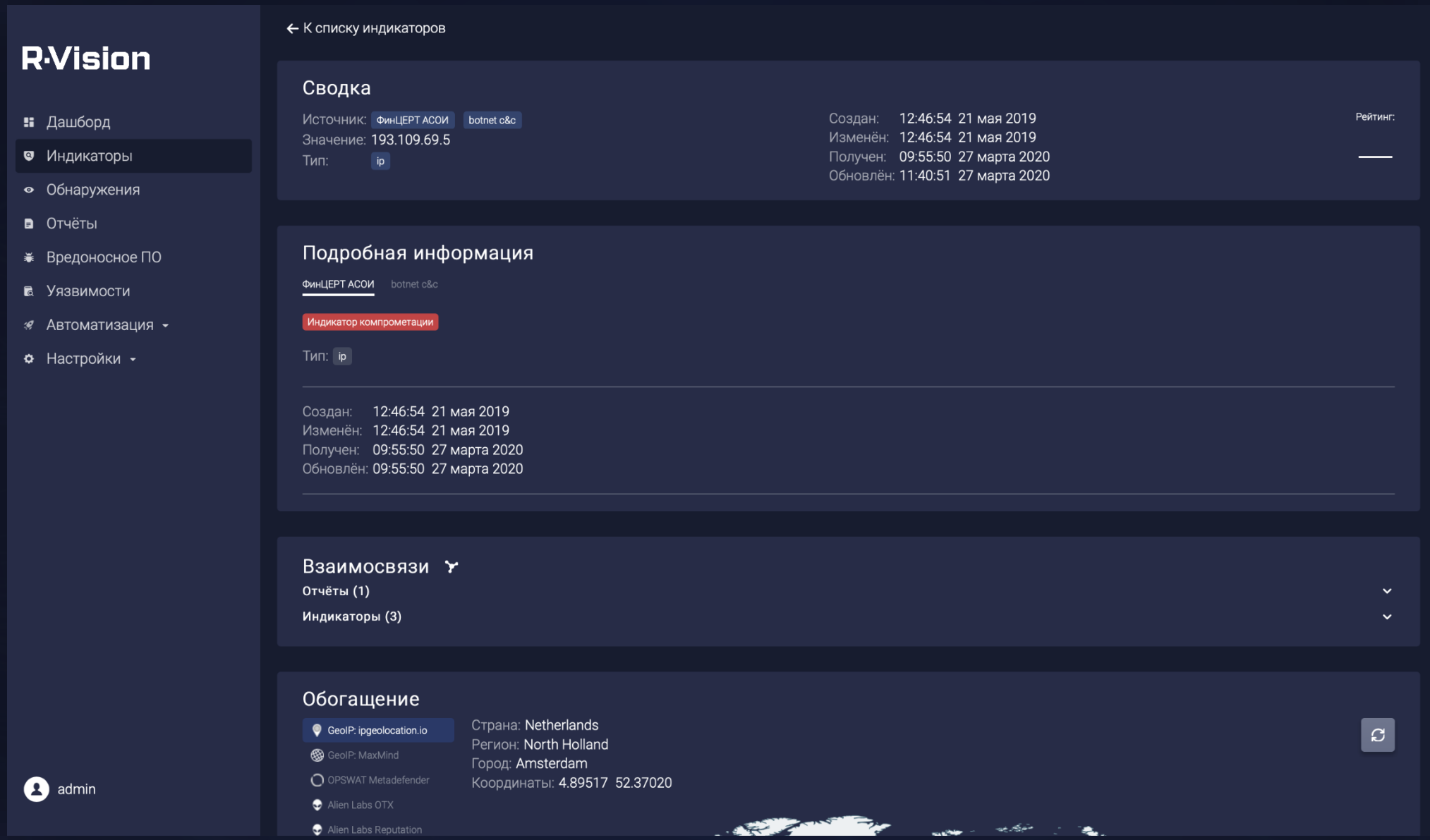
**Оперативное выполнение заданной цепочки действий**



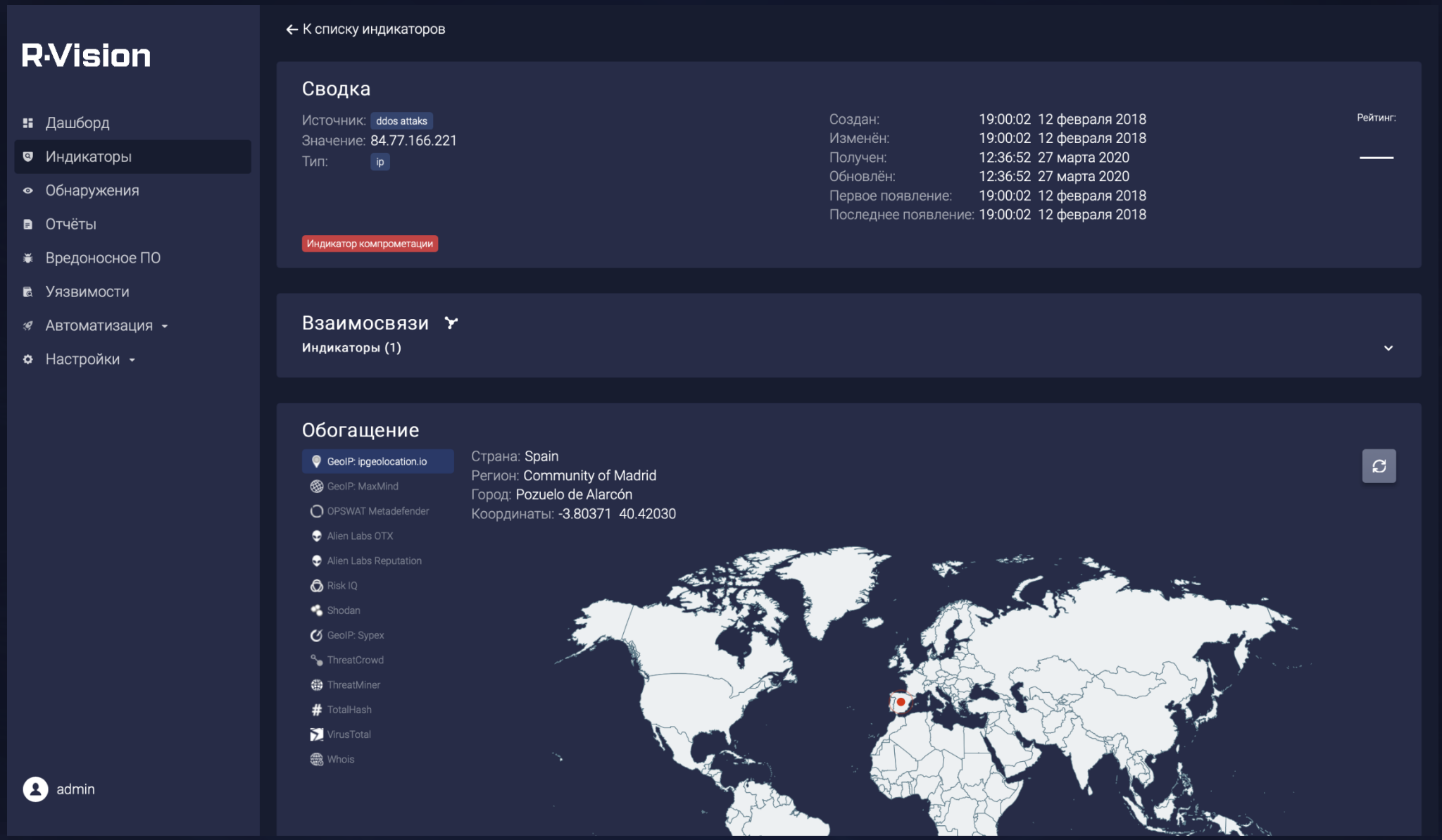



# Источники данных

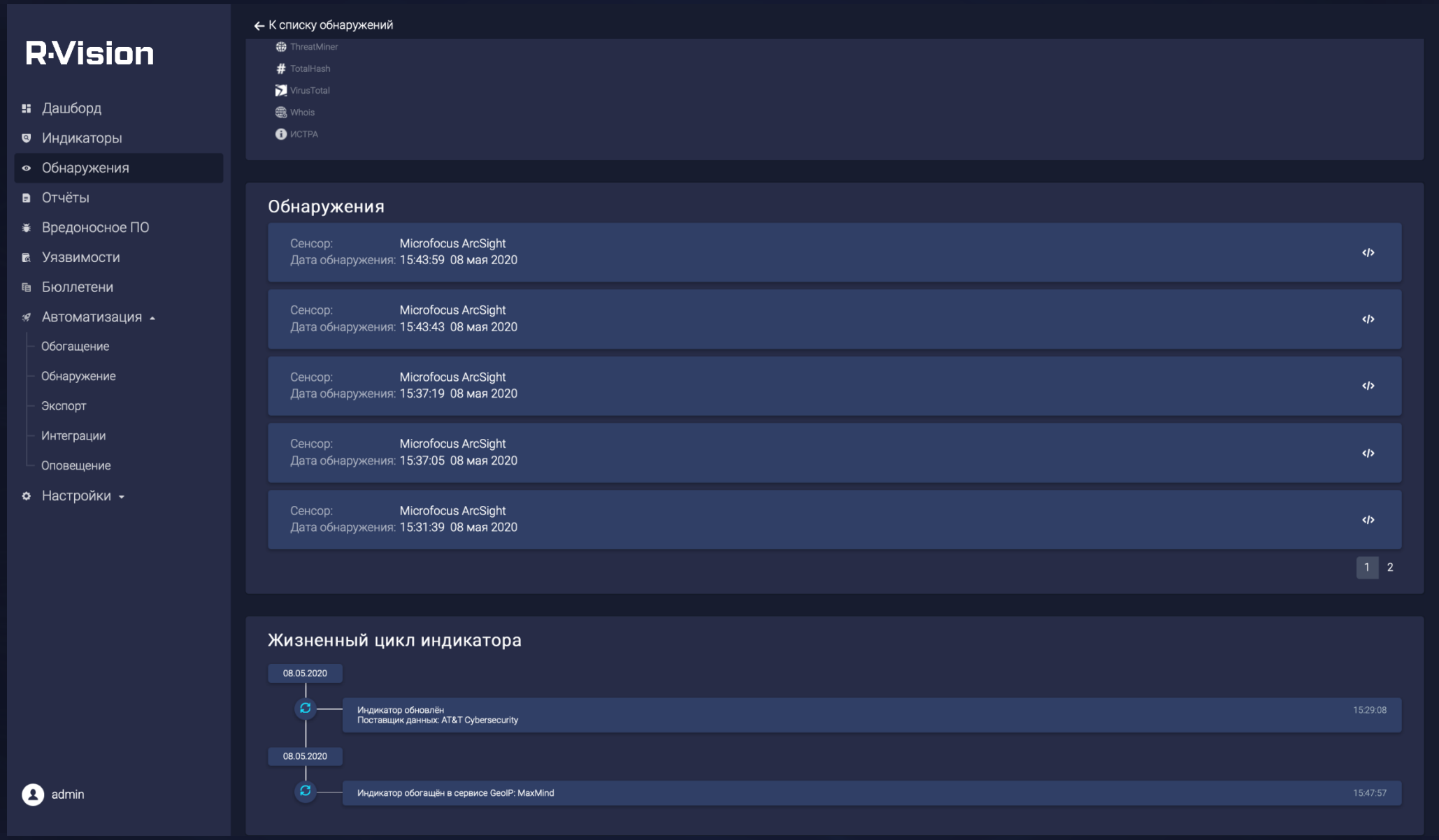

**Единая база индикаторов**



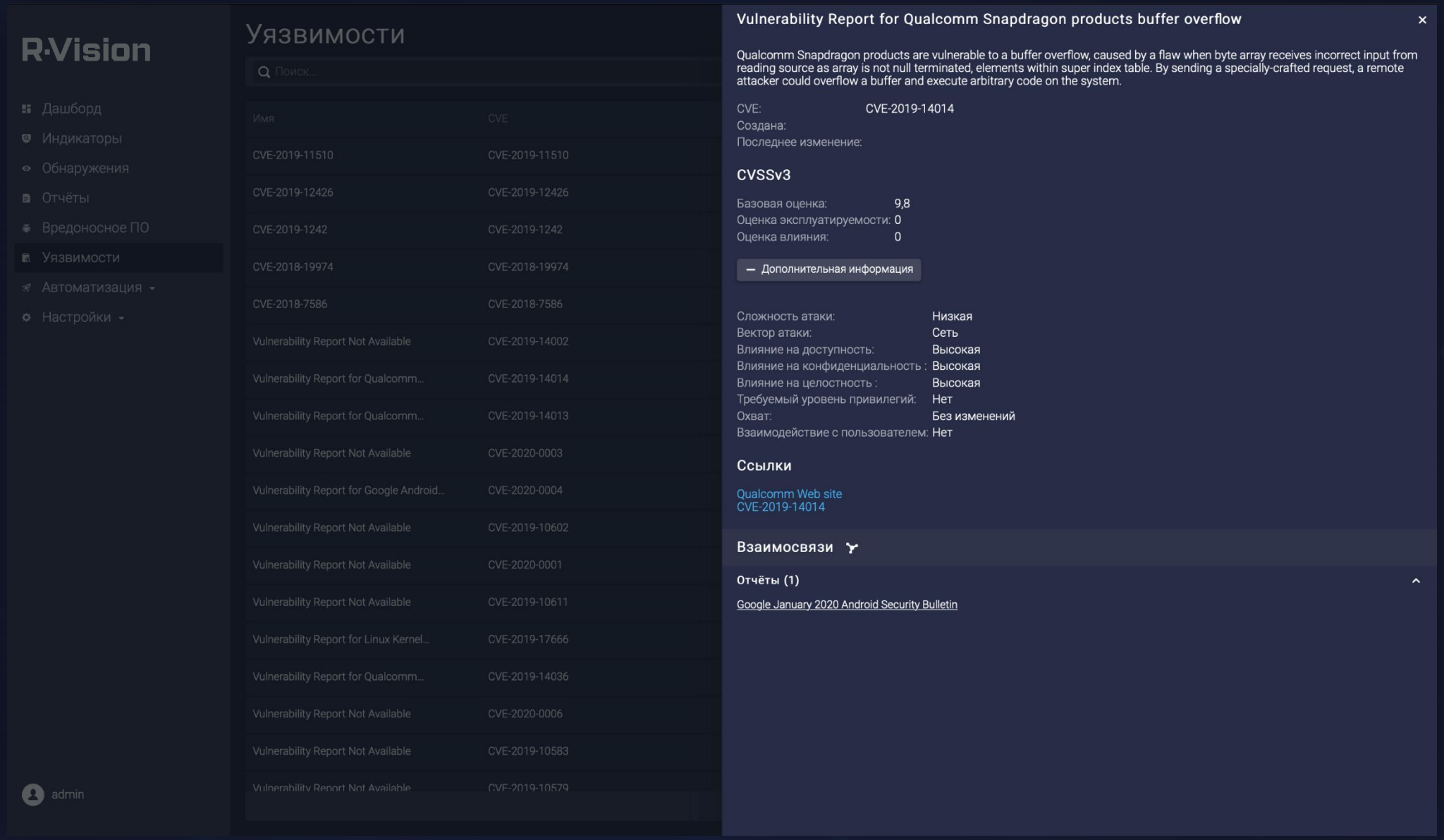

**Карточка индикатора**




## Обогащение индикатора

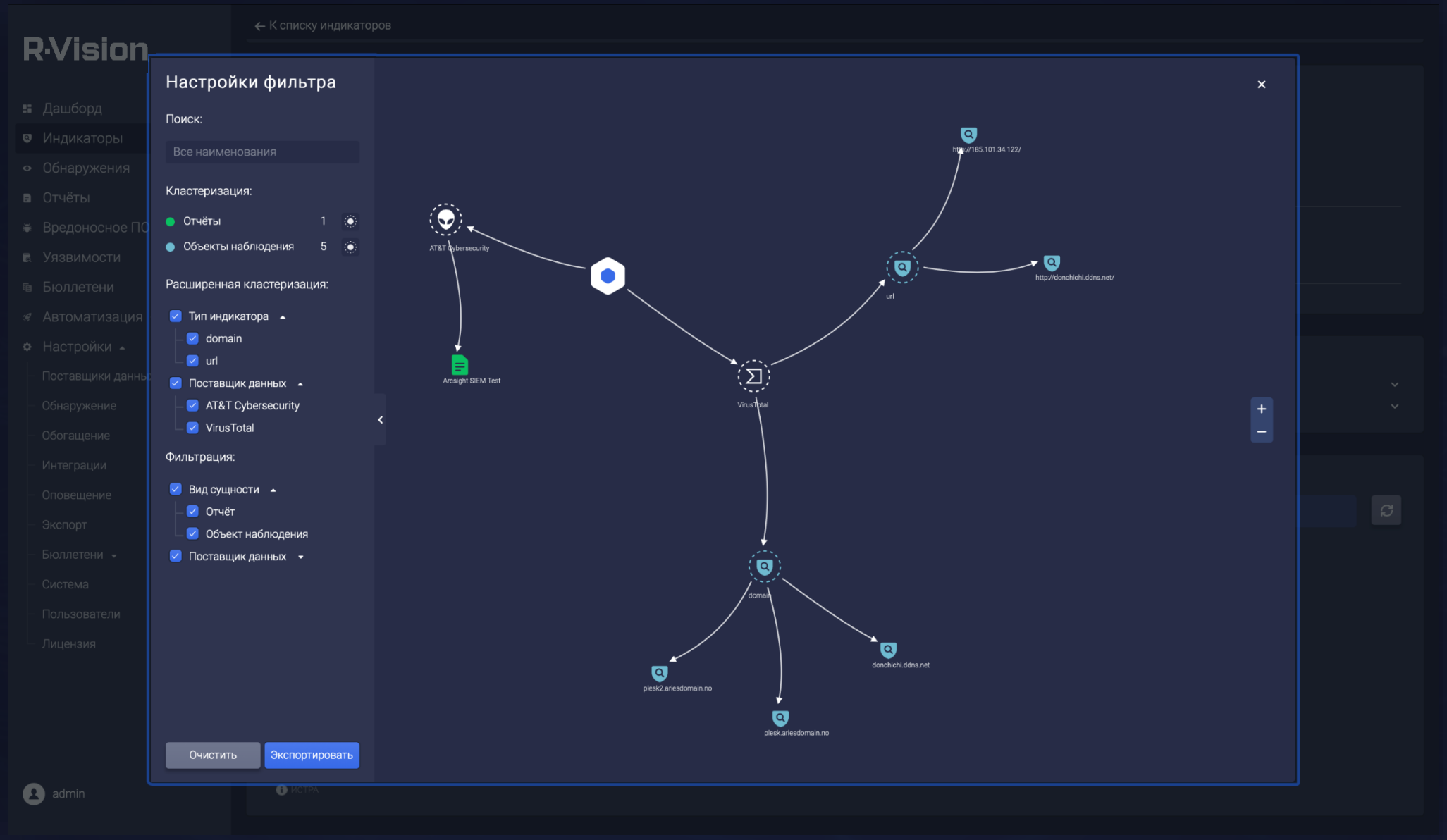



# Обнаружение индикаторов






# Отчеты и взаимосвязи




## Взаимосвязи


## Редактируемый дашборд

# Результат

**Упрощает работу с данными TI,**

**осуществляя непрерывный сбор, нормализацию и хранение данных из различных источников в единой базе**

**Облегчает выявление скрытых угроз,**

**обеспечивая автоматический мониторинг релевантных индикаторов в SIEM с помощью сенсоров**

**Позволяет вовремя блокировать угрозы**

**и минимизировать возможный ущерб благодаря автоматической выгрузке обработанных данных напрямую на СЗИ**

**Ускоряет процессы ИБ**

**за счет быстрого поиска контекста в доступных источниках, анализа связанной информации и автоматизации ключевых сценариев**

# Кейсы использования R-Vision TIP

### Нефтегазовый сектор

**Threat Hunting, выявление и предотвращение APT-атак на ранних этапах в крупной компании нефтегазового сектора**

### Государственный сектор

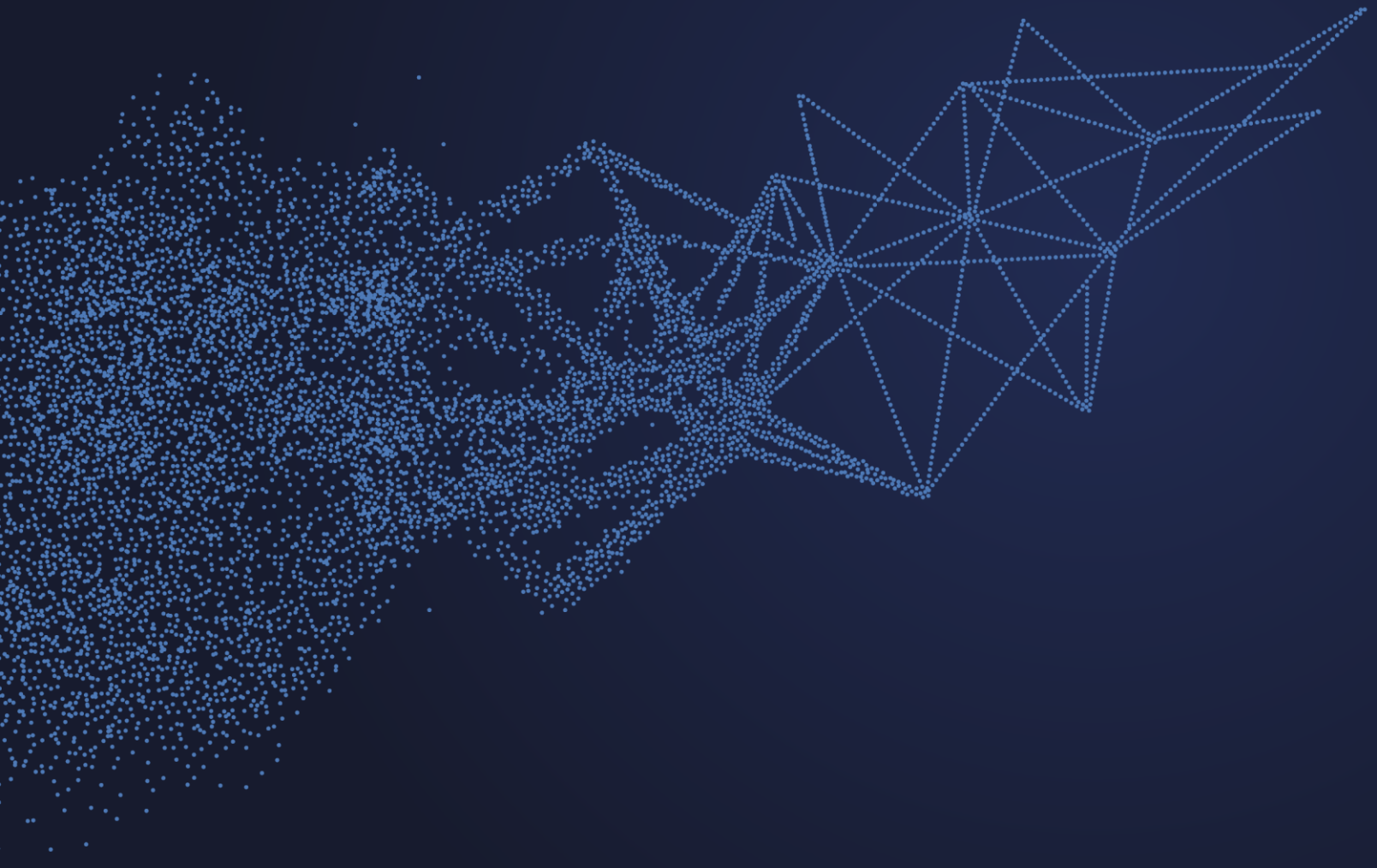
**Автоматическое обнаружение вредоносной активности, связанной с ИТ-активами организаций, которые обслуживаются внешним SOC**

### Финансовый сектор

**Формирование собственных бюллетеней угроз и уязвимостей в ряде крупных российских банков для информирования дочерних структур**

### Промышленный сектор

**Анализ данных об угрозах для повышения эффективности управления уязвимостями, рисками и стратегического планирования в компании промышленного сектора**



R-Vision

+ 7 (499) 322 80 40

sales@rvision.ru

www.rvision.ru

Подписывайтесь на наш дайджест ИБ: rvision.ru/blog