

# PT Threat Analyzer

Как повысить защищенность систем при помощи  
threat intelligence

# Что такое cyberthreat intelligence

- ➔ Cyberthreat intelligence (CTI) — информация, которая описывает **существующие или потенциальные угрозы** безопасности информационных систем и пользователей
- ➔ **Существует в разных формах:**
  - отчеты, содержащие сведения о мотивации, инфраструктуре и техниках определенного злоумышленника
  - IP-адреса, домены, URL и хеш-суммы файлов, связанные с известной угрозой
- ➔ **Используется организациями** для получения контекста событий безопасности и **позволяет быстро отреагировать** на угрозу

# Для чего нам cyberthreat intelligence

# Злоумышленники развиваются

**Обнаружение атак** — критически важная задача, которая с каждым днем становится все сложнее

67%

атак носят целенаправленный характер

96%

организаций не защищены от проникновения внешнего злоумышленника

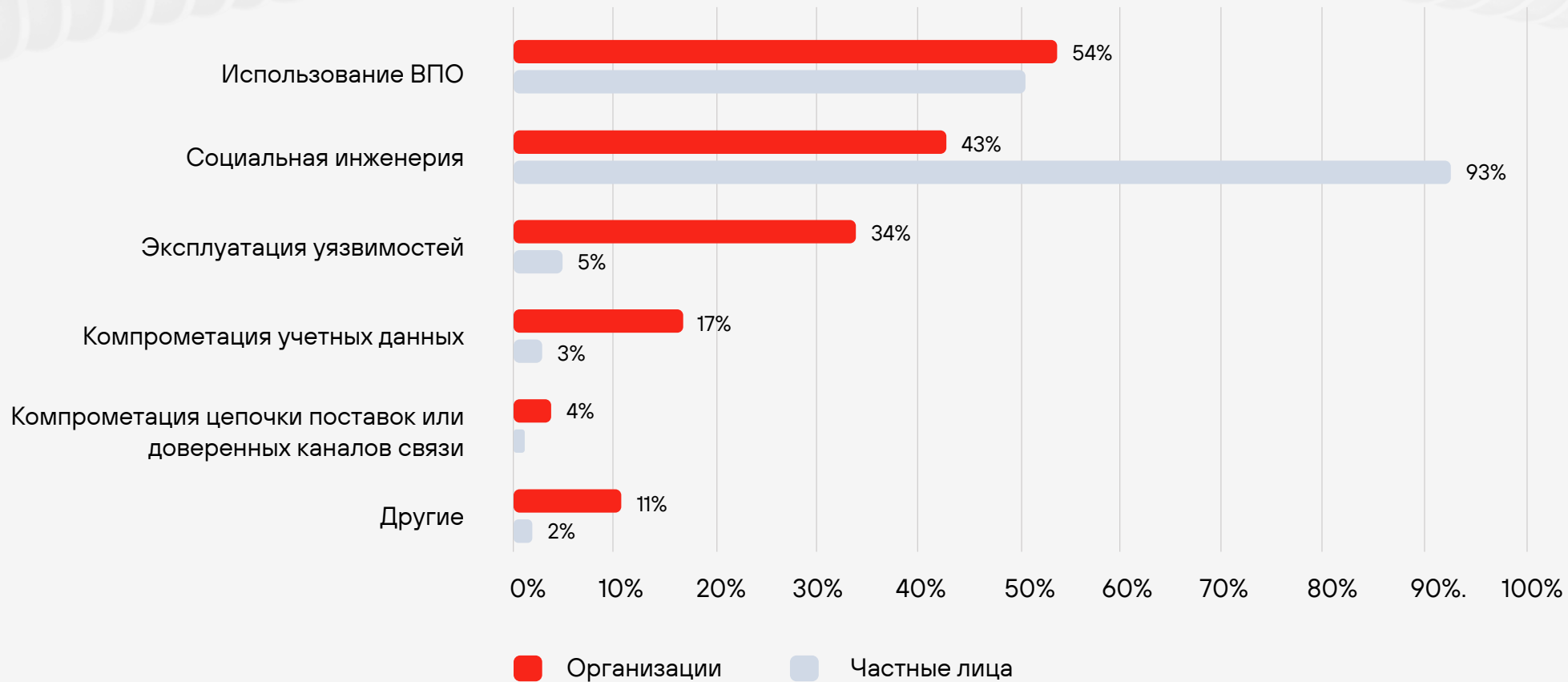
на 20,8%

выросло общее количество инцидентов в 2022 году

в 84%

организаций даже низкоквалифицированный злоумышленник может проникнуть в локальную сеть

# Методы атак по итогам 2022 года

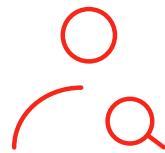


# Реагирование на инциденты неэффективно



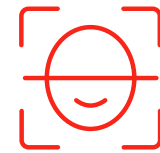
## Развитие технологий

Черви и вирусы меняются быстрее, чем средства защиты могут их обнаружить



## Подкованность злоумышленников

Немалое число группировок пользуются передовыми технологиями, хорошо финансируются и более организованы и мотивированы, чем многие службы защиты информации



## Долгий процесс реагирования

Даже при успешном обнаружении инцидента эксперты могут тратить много времени на уточнение угрозы (кто конкретно атаковал компанию, с какой целью и какие дальнейшие действия может предпринять злоумышленник)

# Что мешает эффективно использовать данные об угрозах

## Отсутствие отлаженного процесса

Сбор, актуализация и распространение знаний об угрозах — сложные задачи, требующие системного подхода

## Применение недостоверной информации

Используя открытые источники данных об угрозах, организации сталкиваются с большим количеством ложных срабатываний

## Нехватка аналитиков

Специалисты по ИБ сталкиваются с необходимостью вручную разбираться с потоком данных об угрозах, приоритизировать их, отсеивать ложные срабатывания и устаревшую информацию

## Отсутствие контекста

Часто данные поставляются без контекста, который позволил бы оценить степень опасности угрозы и помог бы приоритизировать инцидент

## Отсутствие интеграции данных об угрозах

Нарушается комплексность подхода к обеспечению ИБ. Средства защиты пропускают атаки, которые могли быть предотвращены с помощью сведений из других систем

# Как правильно использовать cyberthreat intelligence

# Применение CTI — это процесс, а не проект

**1**

## Планирование

- Какие угрозы релевантны для компании
- Какие субъекты угроз могут потенциально атаковать инфраструктуру компании
- Какие техники, тактики и процедуры (TTP) используются субъектами угроз

**2**

## Сбор данных

Какие источники дадут подходящую и своевременную информацию, а также будут надежными и проверенными

**3**

## Анализ

- Определены ли субъекты угроз, которые могут атаковать инфраструктуру компании
- Определены ли TTP злоумышленников и используемые ими инструменты, а также индикаторы компрометации (IoC)
- Сформированы ли продукты аналитики, готовые к распространению

**4**

## Распространение данных и обратная связь

- Определены ли форматы распространения данных
- Соответствует ли частота распространения периоду, в течение которого контент актуален и максимально востребован
- Предоставлена ли обратная связь по итогам получения данных

# Что предлагает Positive Technologies

# Threat Intelligence

## PT Threat Intelligence Feeds

Потоки данных с индикаторами компрометации

### Предоставление достоверных данных

Содержит сведения об актуальных киберугрозах, собранные экспертами Positive Technologies.

### Повышение эффективности средств защиты

Позволяет обогатить данными используемые системы ИБ, повысить их эффективность и обеспечить обнаружение и предотвращение атак на ранних этапах

## PT Threat Analyzer

Программная платформа для накопления и использования знаний о существующих и потенциальных угрозах информационной безопасности

### Накопление знаний

Получает знания об угрозах из множества разных внутренних и внешних источников, агрегирует их, упорядочивает и выстраивает связи

### Анализ

Позволяет производить гибкий поиск в базе угроз и предоставляет аналитикам подробную информацию об индикаторах компрометации

### Обогащение

Обогащает знания дополнительным контекстом, позволяющим больше узнать о потенциальной угрозе

### Отправка данных в средства защиты

Обеспечивает моментальную доставку и актуализацию знаний

### Собственный TI-сервис

Позволяет формировать собственные потоки данных для распространения в сложных распределенных инфраструктурах

# Как это помогает



## Показываем скрытые угрозы

Позволяем обнаружить атаку на ранних этапах



## Блокируем актуальные угрозы

Проактивно блокируем критически опасные для организации угрозы на периметре



## Ускоряем обработку событий

Экономим время, затрачиваемое на подтверждение, анализ и приоритизацию инцидента



## Автоматизируем

Организуем работу с внешними данными



## Интегрируемся

Автоматизируем доставку данных об угрозах в средства защиты и актуализацию информации



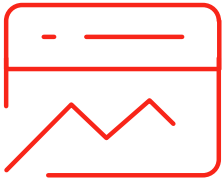
## Предоставляем контекст

Дополняем данные об угрозах

# Результативная кибербезопасность

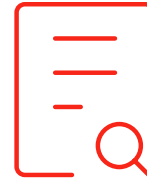
- 1 Оценка практической возможности эксплуатации уязвимостей и угроз
- 2 Формирование перечня недопустимых событий и его регулярное обновление
- 3 Оценка возможности реализации недопустимых событий
- 4 Контроль результативности (эффективности) защиты
- 5 Проведение регулярных практических киберучений
- 6 **Регулярный анализ и оценка новых угроз (threat intelligence)**
- 7 Непрерывное выявление и устранение угроз и уязвимостей
- 8 **Непрерывный мониторинг компьютерных инцидентов и реагирование на них**
- ... И остальное

# Что проводим в рамках методологии результативной кибербезопасности



## Мониторинг инцидентов и реагирование на них

Выстраиваем CTI-процесс, который является неотъемлемой частью мониторинга и реагирования

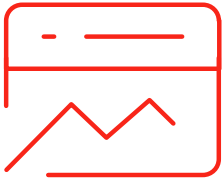


## Регулярный анализ новых угроз

Собираем, поддерживаем в актуальном состоянии, систематизируем, анализируем знания о киберугрозах

# PT Threat Analyzer

Интеграция анализа внешних данных об угрозах в экосистему  
продуктов Positive Technologies



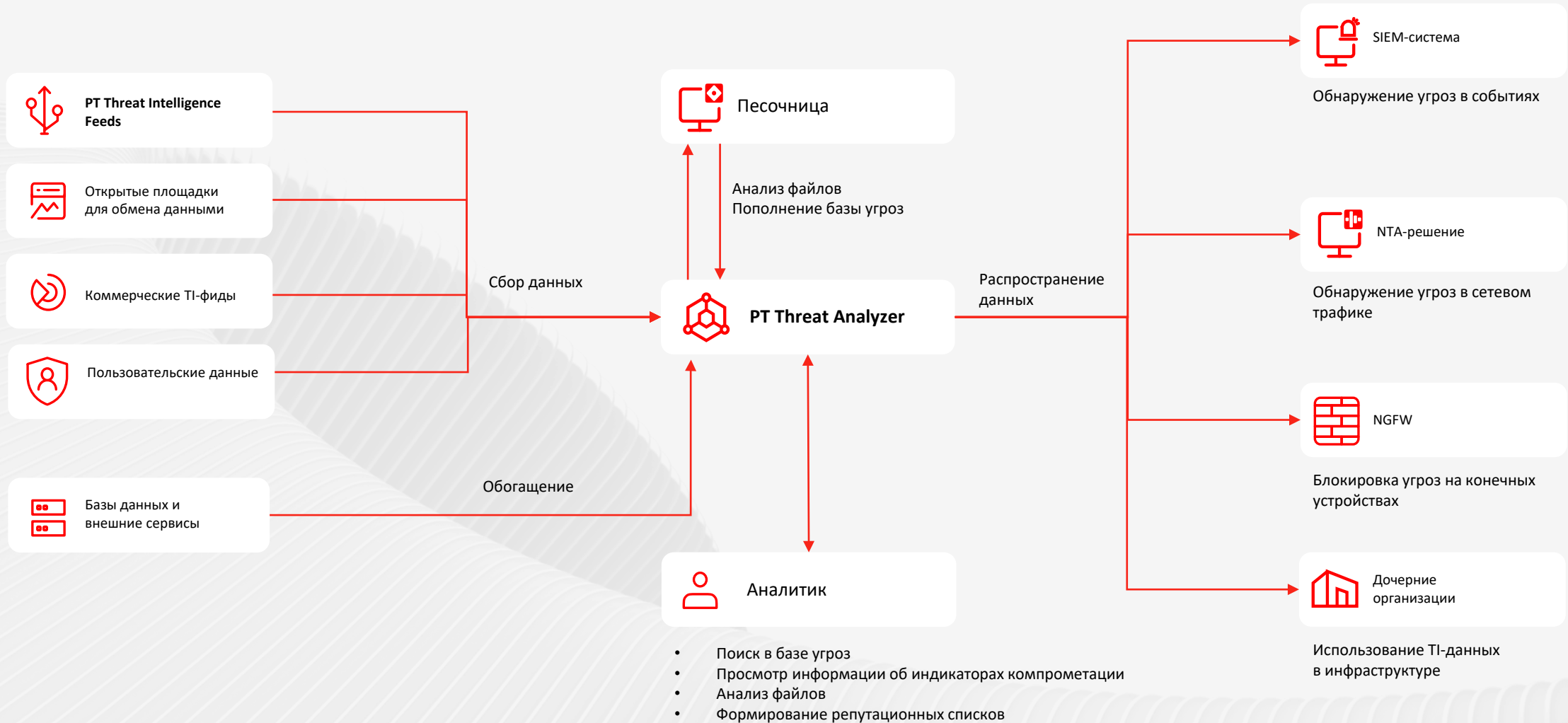
## PT Threat Analyzer

Программная платформа для накопления и использования знаний о существующих и потенциальных угрозах информационной безопасности

Предназначена для интеграции анализа внешних данных об угрозах в экосистему продуктов Positive Technologies

- 1 Сбор**  
данных об угрозах из различных источников
- 2 Обработка**  
поступающих сведений, их нормализация, приведение к единому формату, обогащение дополнительным контекстом. Без предварительной обработки невозможно проанализировать поступающую из разных источников информацию
- 3 Анализ**  
сведений и гибкий поиск в базе данных. Это позволяет аналитикам получать подробную информацию об индикаторах компрометации, оценивать и приоритизировать угрозы
- 4 Распространение**  
информации на средства защиты и другим получателям

# Как работает PT Threat Analyzer



**О продукте**

# Поддерживаемые типы сущностей

## Файл

Информация о файлах, их метаданных и хеш-суммах

## IP-адрес

Свойства IP-адреса. При дополнительной обработке (обогащении) информация дополняется WHOIS- и DNS-записями

## URL

Свойства вредоносного URL или отдельной страницы сайта

## Домен

Свойства доменного имени. При дополнительной обработке (обогащении) информация дополняется WHOIS- и DNS-записями

## Физ. лицо, организация

Идентификационная и контактная информация, а также указание на сферу деятельности участника киберугрозы (жертвы, репортера и т. п.)

## E-mail

Адрес электронной почты, с которого злоумышленники могут рассылать письма, содержащие вредоносные вложения, ссылки, заголовки и т. п.

## Телефон

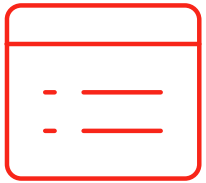
Телефонные номера, связанные с людьми или компаниями

Сущности в PT Threat Analyzer характеризуются наборами атрибутов

Атрибуты могут быть постоянными или меняться с течением времени

Для некоторых атрибутов в качестве значений можно использовать элементы встроенных справочников

# Справочники



**Справочник** — это список названий и описаний, собранных по определенному принципу, позволяющих точнее характеризовать наблюдаемый объект

Связи элементов справочника с объектами в системе позволяют получать качественную аналитику угроз

- Вредоносные кампании
- Злоумышленники
- Классы вредоносного ПО
- Семейства вредоносного ПО
- Сферы деятельности
- Уязвимости

# Достоверность данных

- Факты об объектах и их связях имеют достоверность
- Учитывается информация от всех источников
- Со временем показатель уменьшается

Достоверность факта от 0 до 1 рассчитывается на основании оценки, полученной от источника, и с учетом точности этого источника

Если об одном и том же атрибуте или связи поступают факты от разных источников, PT Threat Analyzer агрегирует эти факты и определяет суммарную достоверность атрибута (связи). Совместимые факты увеличивают показатель, а конфликтующие — уменьшают

Со временем достоверность фактов о динамических атрибутах и связях объекта уменьшается и в какой-то момент становится близкой к нулю. По умолчанию факты хранятся от 5 до 30 дней в зависимости от атрибута (связи)

# Поддерживаемые источники данных

## Пользователи

- Регистрация объектов и их атрибутов в интерфейсе вручную

## Платформы threat intelligence (TIP)

- AlienVault Open Threat Exchange
- Malware Information Sharing Platform

## WHOIS- и DNS-серверы

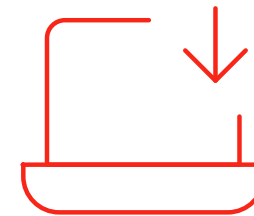
- Обогащение WHOIS- и DNS-записей о доменах и IP-адресах

## Коммерческие поставщики данных

- PT Threat Intelligence Feeds
- RST Threat Feed
- BI.ZONE Threat Intelligence Feed
- Kaspersky Threat Intelligence Feeds

## Анализаторы кода и песочницы

- PT Sandbox
- AVSOFT ATHENA
- Kaspersky Research Sandbox



Архитектура  
продукта позволяет  
подключить любой  
источник  
машиночитаемых  
данных

# Синергия с продуктами Positive Technologies



MaxPatrol SIEM



PT Network Attack  
Discovery



PT Sandbox

# Синергия с продуктами Positive Technologies



MaxPatrol SIEM

Позволяет искать признаки компрометации в событиях безопасности



PT Network Attack  
Discovery

Предоставляет информацию об артефактах в корреляционном событии для подтверждения и приоритизации инцидента



PT Sandbox

# Синергия с продуктами Positive Technologies



MaxPatrol SIEM



PT Network Attack  
Discovery



PT Sandbox

Позволяет искать признаки компрометации в сетевом трафике на основе репутационных списков с индикаторами компрометации

Позволяет получить дополнительную информацию об обнаруженном артефакте

# Синергия с продуктами Positive Technologies



MaxPatrol SIEM



PT Network Attack  
Discovery



PT Sandbox

Передает в PT Threat Analyzer отчеты с результатами статического и динамического анализа файлов

Данные из PT Sandbox пополняют базу индикаторов компрометации в PT Threat Analyzer

# Интеграции с другими системами

## SIEM-системы

- MaxPatrol SIEM
- ArcSight Enterprise Security Manager
- Qradar SIEM

## Межсетевые экраны

- Check Point
- Cisco
- Fortinet
- Palo Alto
- UserGate

## Анализаторы кода и песочницы

- PT Sandbox
- AVSOFT ATHENA
- Kaspersky Research Sandbox



Архитектура продукта позволяет пользователям или интеграторам создавать собственные интеграции благодаря наличию **REST API** и **SDK**

Используется язык Python

# Распространение данных

## Репутационные списки

- Есть выборка данных по определенным условиям
- Информация актуализируется в реальном времени
- Списки предназначены для отправки во внешние системы

## Гибкая фильтрация данных

- Для построения запросов используется встроенный язык
- Учитывается большое количество параметров
- Синтаксис и правила построения запросов описаны в документации

## Настройка объема экспорта данных

- Присутствует механизм для настройки атрибутов, экспортируемых вместе с индикаторами компрометации

# Обогащение данных для внешних систем



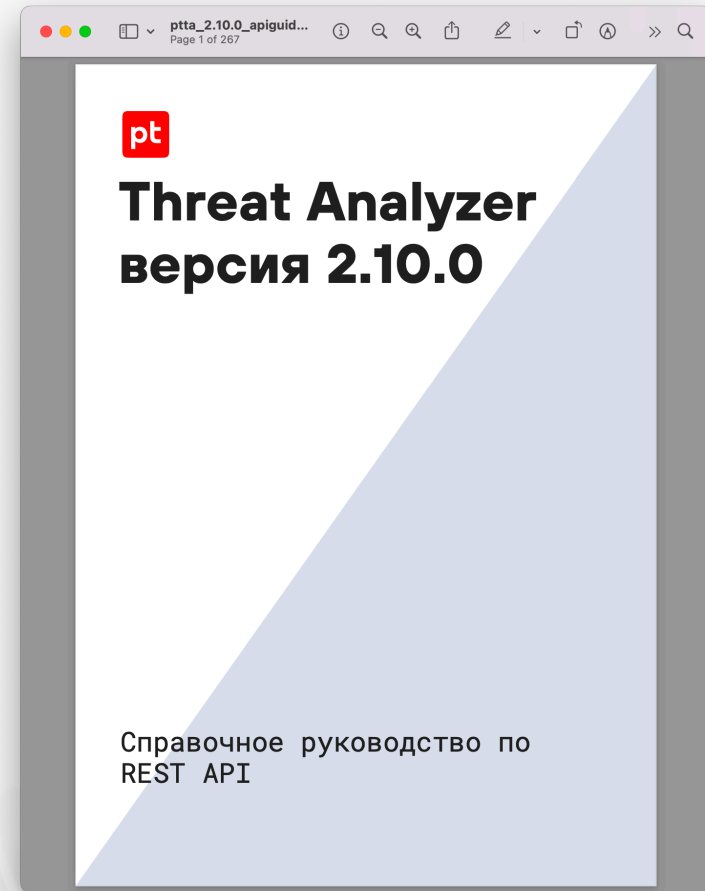
**Источник  
обогащения  
для IRP, SOAR-  
решений и других  
систем**

**REST API позволяет  
как добавлять, так и получать  
информацию:**

- об объектах
- атрибутах
- связях между объектами

# REST API

- Все функции системы доступны через REST API
- В помощь разработчикам предоставляются документация и SDK



# **ОСНОВНЫЕ ВОЗМОЖНОСТИ PT Threat Analyzer**

# Поиск



→ Гибкий поиск в базе угроз

The screenshot displays the Threat Analyzer web application. The main interface shows a table of search results with columns for Type, Object, and Tags. The search filter panel is open on the right, showing various criteria for refining the search.

| Тип      | Объект                                                                                                               | Метки |
|----------|----------------------------------------------------------------------------------------------------------------------|-------|
| URL      | <a href="http://vipcloud-my.xyz/c2sock">http://vipcloud-my.xyz/c2sock</a> <span>IOC</span>                           | tag1  |
| URL      | <a href="http://vipcloud-my.xyz/c2conf">http://vipcloud-my.xyz/c2conf</a> <span>IOC</span>                           |       |
| URL      | <a href="http://vipcloud-my.xyz">http://vipcloud-my.xyz</a> <span>IOC</span>                                         |       |
| Домен    | <a href="http://vipcloud-my.xyz">vipcloud-my.xyz</a>                                                                 |       |
| IP-адрес | <a href="http://195.178.120.24">195.178.120.24</a> <span>IOC</span>                                                  |       |
| URL      | <a href="http://195.178.120.24/droidftpmabase64.txt">http://195.178.120.24/droidftpmabase64.txt</a> <span>IOC</span> |       |

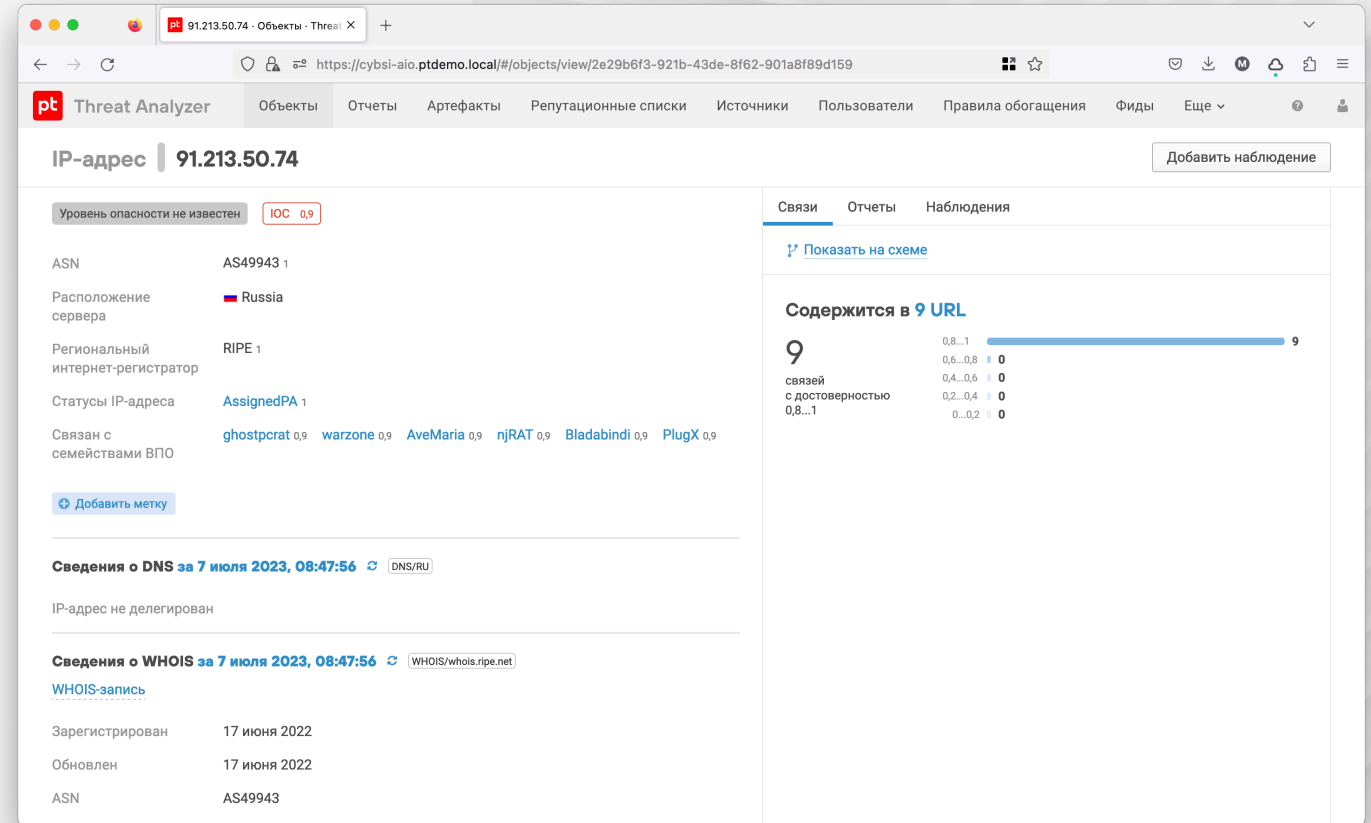
**Расширенный поиск** | Сохраненные фильтры

- Тип объекта:
- Степень опасности:
- ☐ Является индикатором компрометации
- ☐ Исключить доверенные
- Уровень доступа:
- Метки:
- Источники:
- Роль узла в сети:

[Сохранить фильтр](#) [Применить](#) [Сбросить](#)

# Карточка индикатора компрометации

→ Подробная информация об индикаторах компрометации для аналитиков



The screenshot displays the Threat Analyzer web interface. The main header shows the IP address 91.213.50.74. Below this, a table lists various attributes of the IP, including its ASN (AS49943), location (Russia), regional internet registry (RIPE), and status (AssignedPA). A section titled 'Сведения о DNS' shows that the IP is not delegated. Another section titled 'Сведения о WHOIS' shows that the IP was registered and updated on June 17, 2022. On the right side, a 'Содержится в 9 URL' section displays a bar chart showing the number of URLs containing the IP address, with a total of 9 URLs.

| Атрибут                           | Значение                                                |
|-----------------------------------|---------------------------------------------------------|
| ASN                               | AS49943                                                 |
| Расположение сервера              | Russia                                                  |
| Региональный интернет-регистратор | RIPE                                                    |
| Статусы IP-адреса                 | AssignedPA                                              |
| Связан с семействами ВПО          | ghostpcrat, warzone, AveMaria, njRAT, Bladabindi, PlugX |

Сведения о DNS за 7 июля 2023, 08:47:56

IP-адрес не делегирован

Сведения о WHOIS за 7 июля 2023, 08:47:56

WHOIS-запись

| Атрибут         | Значение     |
|-----------------|--------------|
| Зарегистрирован | 17 июня 2022 |
| Обновлен        | 17 июня 2022 |
| ASN             | AS49943      |

Содержится в 9 URL

| Связи с достоверностью | 0,8...1 |
|------------------------|---------|
| 0,8...1                | 9       |
| 0,6...0,8              | 0       |
| 0,4...0,6              | 0       |
| 0,2...0,4              | 0       |
| 0...0,2                | 0       |

# Отчеты



Поиск и просмотр отчетов,  
которые содержат данные  
об объектах

PT Threat Analyzer

Объекты

Отчеты

Артефакты

Репутационные списки

Источники

Пользователи

Правила обогащения

Фиды

Еще

Отчет PT Sandbox scan from retro

Уровень доступа

Зарегистрирован в PT Threat Analyzer

Дата создания

Обновлен в PT Threat Analyzer

Источник

Автор изменений

Внешний ресурс

Amber

5 июля 2023 19:42

5 июля 2023

5 июля 2023 19:42

PT Sandbox Malware Report/Malware Report

PT Sandbox Malware Report/Malware Report

<https://sandbox.ptdemo.local/tasks/290b82dc-1b53-11ee-802a-04ecd1f9e862>

Общие сведения за 5 июля 2023, 19:42:38

Источник

Автор изменений

PT Sandbox Malware Report/Malware Report

PT Sandbox Malware Report/Malware Report

Файл: [bc21f289cc113a77ca1f48900a321d8f0eff024634a9255becc8afda66c213bd](#)

Атрибуты

Вредоносное ПО 1

Размер

77,82 KB 1

IOC 1

Классы ВПО

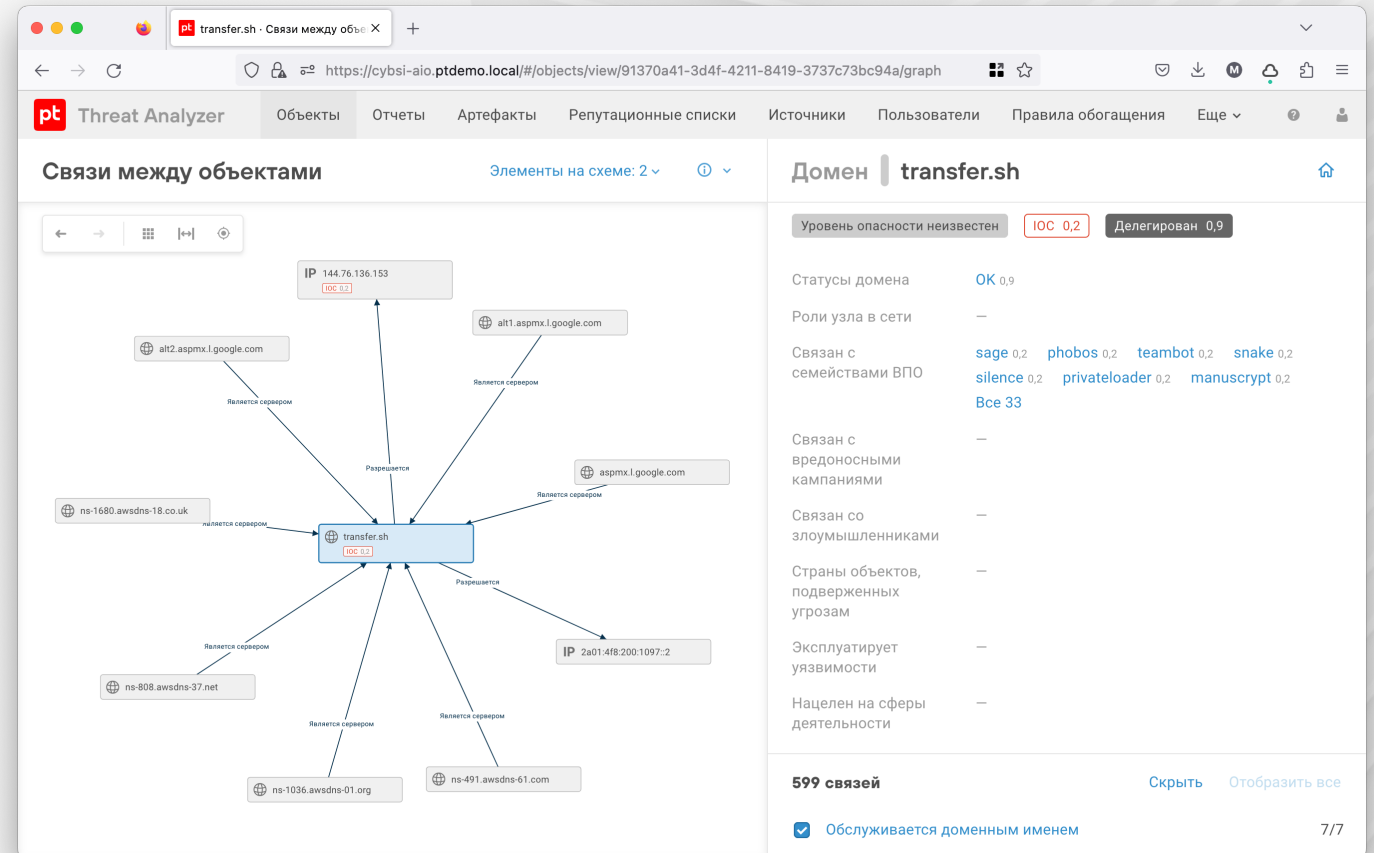
Похожие отчеты

Источник

| Название                                        | Источник                | Создан               |
|-------------------------------------------------|-------------------------|----------------------|
| <a href="#">PT Sandbox scan from PTDemo-XDR</a> | PT Sandbox (PT Multi... | 4 июля 2023 19:45:35 |

# Граф связей

→ Визуализация связей между объектами в системе



# Анализ файлов

→ Отправка файла на поведенческий анализ в песочницу. Это позволяет моделировать поведение вредоноса в виртуальном окружении, изолированном от информационной системы организации

pt

2a1d2761bbf26e72fb719a68b3... X

pt Не указано - Отчеты - Threat A X

+

← → ↺

🔒 https://cybsi-aiو.ptdemo.local/#/reports/view/04961552-5a10-40f0-946e-44176b140a28

🗖 ⭐

📧 ⬇ Ⓜ ⚙ 📄 ⌵

pt Threat Analyzer

Объекты

Отчеты

Артефакты

Репутационные списки

Источники

Пользователи

Правила обогащения

Еще ▾

🔍 👤

Отчет Не указано

Уровень доступа

🔒 Amber

Зарегистрирован в PT Threat Analyzer

11 июля 2023 12:08

Дата создания

11 июля 2023

Обновлен в PT Threat Analyzer

11 июля 2023 12:08

Источник

PT Sandbox (PT MultiScanner)/Local

Автор изменений

PT Sandbox (PT MultiScanner)/Local

Внешний ресурс

<https://192.168.53.1/tasks/bc50ef18-1fca-11ee-90ad-00d18300...> 🔗

🔒 Общие сведения за 11 июля 2023, 12:08:39

Источник

PT Sandbox (PT MultiScanner)/Local

Автор изменений

PT Sandbox (PT MultiScanner)/Local

Файл: **1 2a1d2761bbf26e72fb719a68b35df6baeca56a641e8a7a8f06c79941116c...** IDC

Атрибуты

Размер

181 В 1

Классы ВПО

Backdoor 1

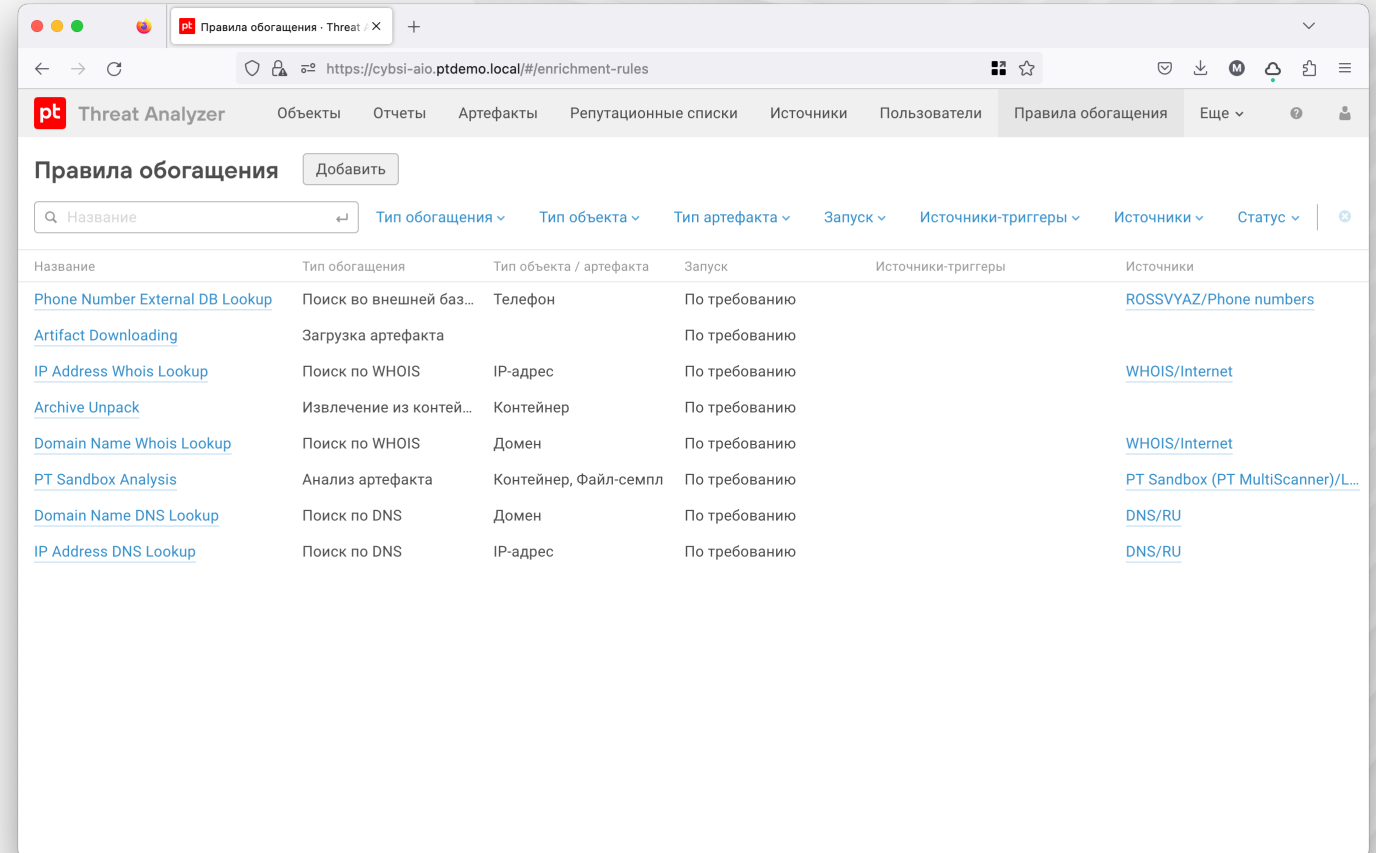
Похожие отчеты

Источник ▾

| Название                                        | Источник                | Создан                |
|-------------------------------------------------|-------------------------|-----------------------|
| <a href="#">PT Sandbox scan from ptnad</a>      | PT Sandbox Malware ...  | 5 июля 2023 17:45:45  |
| <a href="#">PT Sandbox scan from cybsi-demo</a> | PT Sandbox Malware ...  | 6 июля 2023 15:44:53  |
| <a href="#">Не указано</a>                      | PT Sandbox (PT Multi... | 6 июля 2023 15:44:55  |
| <a href="#">PT Sandbox scan from cybsi-demo</a> | PT Sandbox Malware ...  | 7 июля 2023 11:43:16  |
| <a href="#">Не указано</a>                      | PT Sandbox (PT Multi... | 7 июля 2023 11:43:17  |
| <a href="#">PT Sandbox scan from retro</a>      | PT Sandbox Malware ...  | 8 июля 2023 11:43:36  |
| <a href="#">PT Sandbox scan from retro</a>      | PT Sandbox Malware ...  | 8 июля 2023 11:43:35  |
| <a href="#">PT Sandbox scan from cybsi-demo</a> | PT Sandbox Malware ...  | 11 июля 2023 12:08:38 |

# Правила обогащения

→ Обогащение данных в соответствии со встроенными или пользовательскими правилами. Такие правила позволяют автоматически или вручную создавать задачи на обогащение объекта или артефакта в указанном источнике

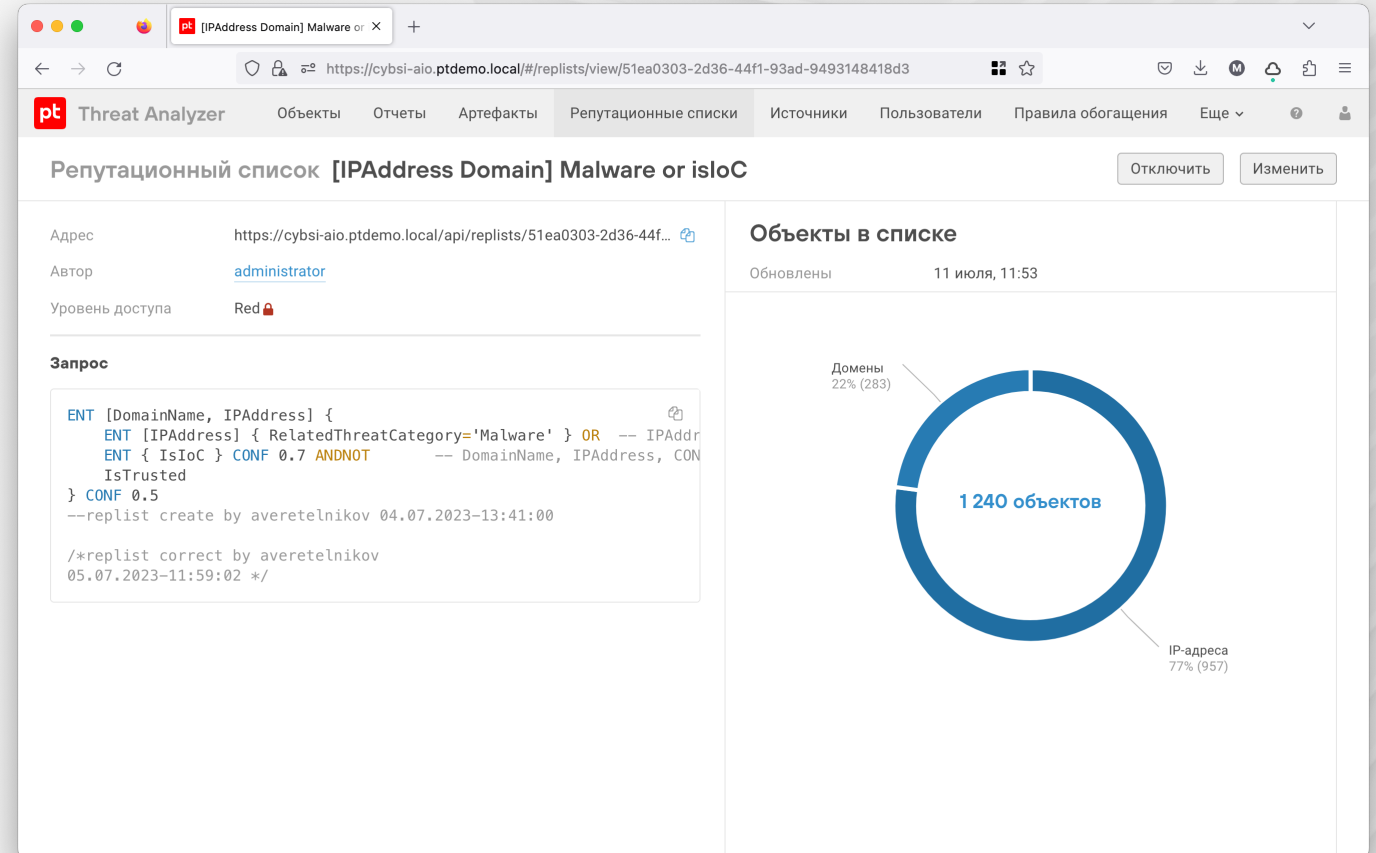


| Название                                        | Тип обогащения          | Тип объекта / артефакта | Запуск        | Источники-триггеры | Источники                                         |
|-------------------------------------------------|-------------------------|-------------------------|---------------|--------------------|---------------------------------------------------|
| <a href="#">Phone Number External DB Lookup</a> | Поиск во внешней баз... | Телефон                 | По требованию |                    | <a href="#">ROSSVYAZ/Phone numbers</a>            |
| <a href="#">Artifact Downloading</a>            | Загрузка артефакта      |                         | По требованию |                    |                                                   |
| <a href="#">IP Address Whois Lookup</a>         | Поиск по WHOIS          | IP-адрес                | По требованию |                    | <a href="#">WHOIS/Internet</a>                    |
| <a href="#">Archive Unpack</a>                  | Извлечение из контей... | Контейнер               | По требованию |                    |                                                   |
| <a href="#">Domain Name Whois Lookup</a>        | Поиск по WHOIS          | Домен                   | По требованию |                    | <a href="#">WHOIS/Internet</a>                    |
| <a href="#">PT Sandbox Analysis</a>             | Анализ артефакта        | Контейнер, Файл-семпл   | По требованию |                    | <a href="#">PT Sandbox (PT MultiScanner)/L...</a> |
| <a href="#">Domain Name DNS Lookup</a>          | Поиск по DNS            | Домен                   | По требованию |                    | <a href="#">DNS/RU</a>                            |
| <a href="#">IP Address DNS Lookup</a>           | Поиск по DNS            | IP-адрес                | По требованию |                    | <a href="#">DNS/RU</a>                            |

# Репутационные списки

→ Группировка объектов по общим признакам в соответствии с запросом, написанным на специализированном языке. Такая группа объектов называется репутационным списком. Он может включать, например, все вредоносные объекты, существующие в системе, или все IP-адреса (домены), являющиеся Торг-узлами

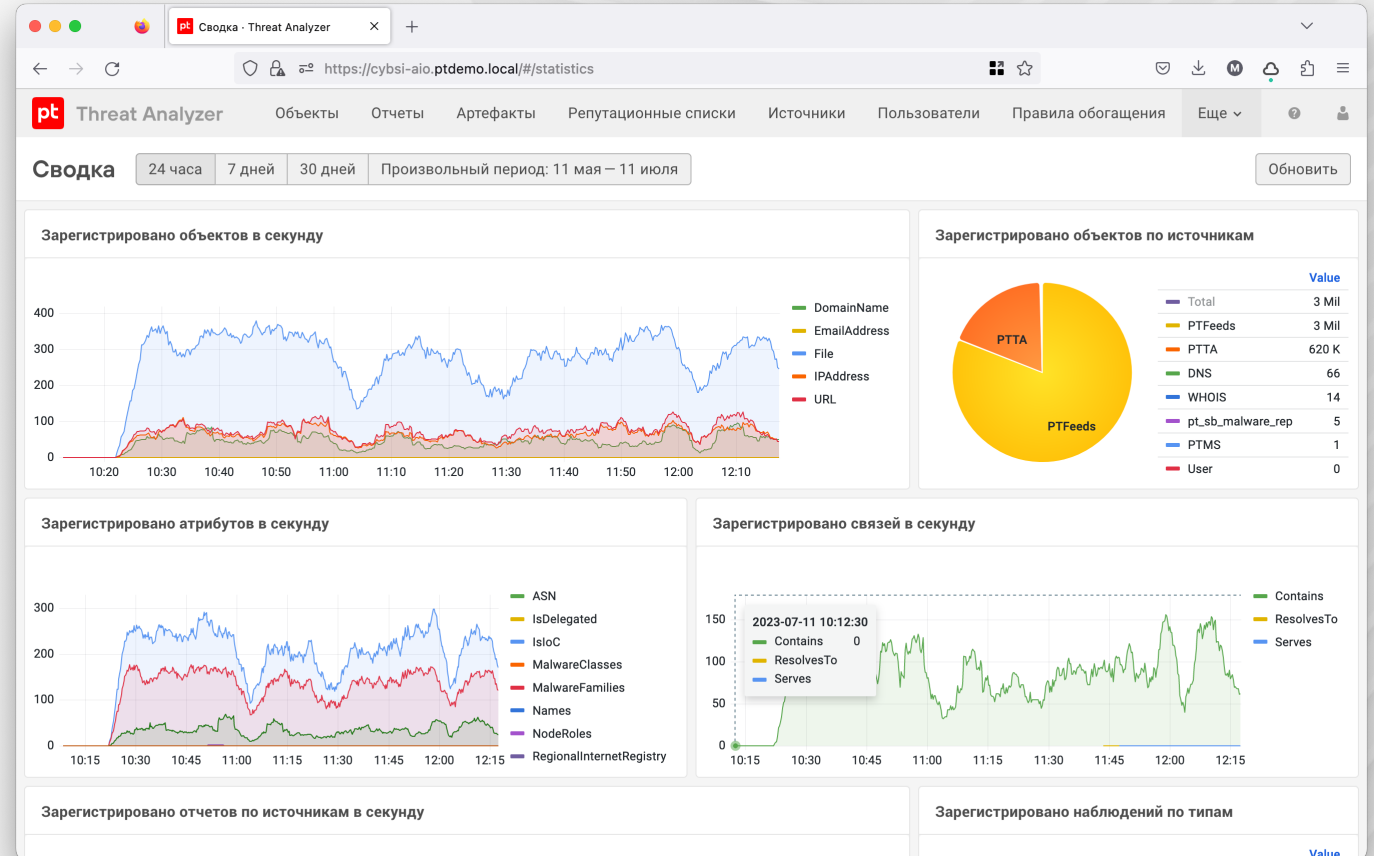
Репутационные списки обновляются в реальном времени



# Сводка



→ На странице «Сводка» в панелях с графиками и диаграммами — отображение статистики регистрации и обогащения данных в системе



**Спасибо!**