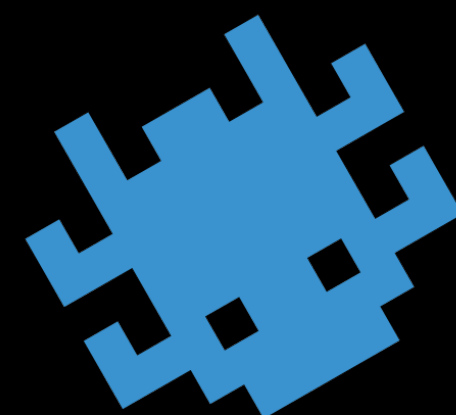




# Netlas.io

## ТЕХНИЧЕСКИЙ АТЛАС ИНТЕРНЕТА

*Netlas.io – это поисковая система по устройствам и службам, составляющим всемирную сеть*

*Котылевский Артур Суренович  
Генеральный директор, ООО “Нетлас”, г. Санкт-Петербург*



# Инструмент помогает решать следующие проблемы:

| Проблема                                                        | В чем сложность?                                                                                                                                         | Как помогает <a href="#">Netlas.io</a> ?                                                                                                                |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| ♦ <i>Идентифицировать поверхность атаки*</i>                    | Технически сложная задача, требует высокой квалификации, на решение уходят дни                                                                           | ✓ Автоматическое построение поверхности атаки                                                                                                           |
| ♦ <i>Выполнить аудит безопасности, выявить уязвимые ресурсы</i> | Современные решения автоматизации аудита не умеют идентифицировать сетевой периметр, нужны высококвалифицированные кадры                                 | ✓ Ежедневный аудит безопасности может выполнять персонал с минимальными компетенциями в ИБ                                                              |
| ♦ <i>Следить за изменениями поверхности атаки</i>               | Чтобы собрать информацию, которую предоставляет <a href="#">Netlas.io</a> , нужно обратиться <u>как минимум к трем</u> разным платным источникам данных. | ✓ <a href="#">Netlas.io</a> автоматически выявляет новые компоненты поверхности атаки, такие как домены, сети, хосты, в т.ч. так называемое Shadow IT** |

\* Англоязычный термин – attack surface.

\*\* Неучтенные ресурсы, неизвестные службе IT или ИБ, ошибочно опубликованные службы и сервисы.

# Актуальность проблемы

Согласно исследованию\* 208 компаний со штатом от 5 000 человек:

**93%** выбрали своим главным приоритетом на ближайшие годы идентификацию и мониторинг поверхности атаки.

**53%** отметили «необходимость защитить всю поверхность атаки, поскольку сложно/невозможно оценить критичность отдельных компонентов.

**65%** сообщили об отсутствии кадров с достаточной для решения этой задачи квалификацией.

Отсутствие прозрачности связано по большей части с возможностями инструментов, которые используют организации.

\* Исследование Censys от 28.06.2023 - <https://www.csoonline.com/article/643881/attack-surface-visibility-a-top-ciso-priority-amid-growing-attacks-report.html>



# Netlas.io позволяет:

- ✓ находить различные устройства и сервисы, например, IoT-устройства, промышленное оборудование, вредоносное ПО;
- ✓ исследовать отдельные узлы и целые сети, находить взаимосвязи;
- ✓ мониторить совокупности объектов, например, ЦОД или сетевой периметр компании;
- ✓ исследовать безопасность совокупности устройств;
- ✓ приобретать библиотеки данных.

The screenshot displays the Netlas.io web application interface. At the top, there's a navigation bar with 'Netlas.io', 'Search', 'Datastore', 'Pricing', and 'API'. A search bar contains 'sk.ru'. Below the search bar, the results for 'sk.ru' are shown, including A records, Whois data, Related domains, MX records, and NS records. The 'Exposed ports & software' section is expanded, showing a table of ports, protocols, URIs, tags (software), and CVEs.

| Port | Protocol* | URI                                | Tags (software)                                   | CVE                                                  |
|------|-----------|------------------------------------|---------------------------------------------------|------------------------------------------------------|
| 80   | http      | http://sk.ru:80/                   | nginx                                             | -                                                    |
| 443  | https     | https://sk.ru:443/                 | nginx                                             | -                                                    |
| 443  | https     | https://contractors.sk.ru:443/owa/ | iis (10.0) microsoft_aspnet<br>microsoft_exchange | -                                                    |
| 443  | https     | https://live.sk.ru:443/            | 1c_bitrix nginx php (5.6.40) youtube              | CVE-2019-9641 CVE-2017-8923 CVE-2017-9225 13 more... |
| 443  | https     | https://visa.sk.ru:443/            | 1c_bitrix nginx (1.16.1) php (7.2.33)             | CVE-2020-7869 CVE-2022-31638 CVE-2017-8923 3 more... |
| 443  | https     | https://webvpn.sk.ru:443/          | cisco_anyconnect_vpn                              | -                                                    |
| 80   | http      | http://zakupki.sk.ru:80/           | nginx                                             | -                                                    |

This screenshot shows a detailed view of a specific IP address in the Netlas.io interface. It includes a map of the IP's location, a list of associated domains, and a detailed view of the IP's history and associated data.

This screenshot displays a network graph visualization within the Netlas.io interface. The graph shows various nodes representing IP addresses and domains, connected by lines indicating relationships or data flows between them.

This screenshot shows a list of IP addresses and their associated data in the Netlas.io interface. The list includes columns for IP address, associated domains, and other relevant information, presented in a tabular format.

# Netlas.io взаимодействует с каждым доступным в Интернет узлом

~ **4** млрд.  
IP-адресов

~ **2,5** млрд.  
записей DNS

> **5** млрд.  
сертификатов

~ **11** млн.  
подсетей

~ **400** млн.  
доменов (TLD)

Для каждого ресурса **Netlas.io** собирает:

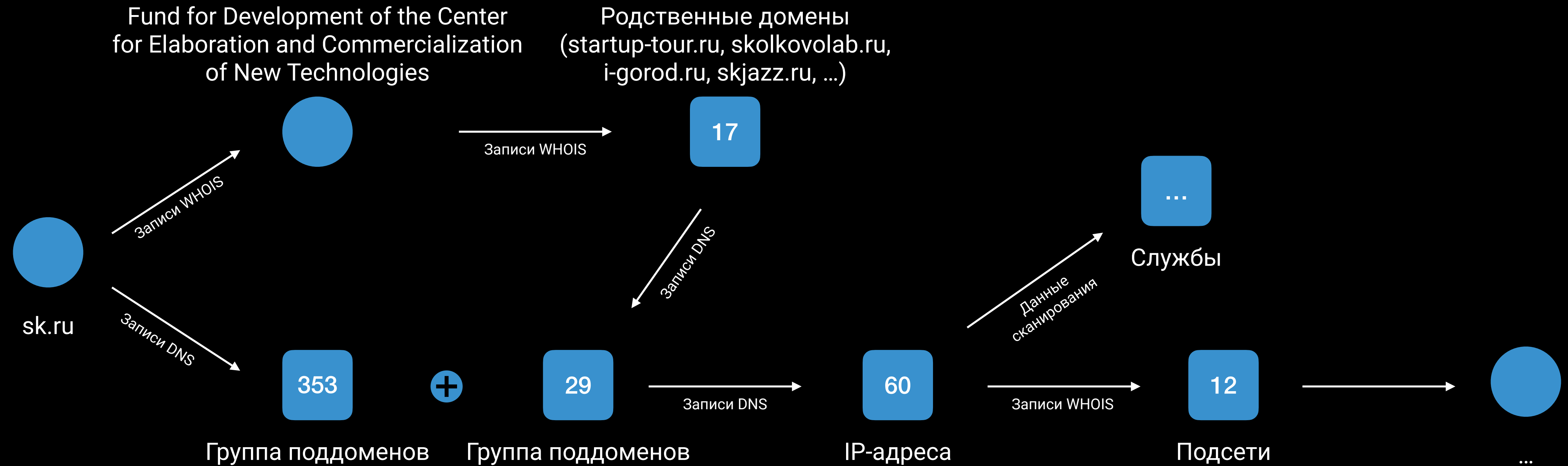
## Результаты сканирования IP-адресов и сайтов

- полный ответ сервера
- продукты, используемые технологии и типы устройств
- данные о безопасности  
(является ли этот узел VPN или иным анонимайзером, есть ли уязвимости, фигурирует ли в списках вредоносных ресурсов)

## Данные от регистраторов и провайдеров

- наименование и контакты компании-владельца;
- геолокация, включая страну, город, индекс и часовой пояс;
- наименование и контакты провайдера;
- информацию о подсети и множество прочей технической информации

# Инструмент визуализации поверхности атак



- ✓ Простая, удобная и наглядная форма взаимодействия с приложением, существенно снижает требования к квалификации пользователя.
- ✓ Специалисту не нужно знать ничего, кроме домена организации.
- ✓ В дальнейшем система подскажет об изменении поверхности атаки.

# Мониторинг поверхности атаки

⌚ (в разработке)

- ✓ Ежедневное сканирование поверхности атаки
- ✓ Сканирование из разных геолокаций
- ✓ Изменения в сравнении с предыдущими результатами
- ✓ Выявленные уязвимости и недостатки конфигурации



- ✓ Выявление изменений состава поверхности атаки (появление новых доменных имен, подсетей, выявление новых поддоменов, изменения в записях DNS)
- ✓ Выявление т.н. Shadow IT и фишинговых ресурсов

# Сравнение Netlas.io с конкурентами

| Технико-экономические параметры              |  Shodan.io |  Censys.io |  Criminalip.io |  Netlas.io |
|----------------------------------------------|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Уникальных посетителей, штук в месяц         | 559 430                                                                                       | 203 837                                                                                       | 57 912                                                                                            | 8 572                                                                                         |
| Количество результатов сканирования Интернет | 789 998 518                                                                                   | 293 531 204                                                                                   | 109 591 223                                                                                       | 905 768 268                                                                                   |
| Особенности сканирования                     | IPv4, IPv6, домены                                                                            | IPv4, IPv6                                                                                    | IPv4                                                                                              | IPv4, домены                                                                                  |
| Количество данных на результат               | объем ответа ограничен                                                                        | сохраняется полный ответ сервера                                                              | сохраняется полный ответ сервера                                                                  | сохраняется полный ответ сервера                                                              |
| Средняя актуальность данных                  | ~5 дней                                                                                       | 1 день                                                                                        | ~15 дней                                                                                          | ~15 дней                                                                                      |
| Дополнительные библиотеки                    | Домены                                                                                        | Нет                                                                                           | Abuse records                                                                                     | Домены, whois                                                                                 |
| Обогащение                                   | GeoIP, технологии, CVE                                                                        | GeoIP, технологии, CVE                                                                        | GeoIP, технологии, CVE                                                                            | GeoIP, технологии, CVE whois                                                                  |
| Позиционирование                             | Threat Intelligence + Monitoring                                                              | Attack Surface Management + Threat Intelligence                                               | Threat Intelligence                                                                               | Threat Intelligence + AUTOMATIC Attack Surface Management                                     |

\* По состоянию на март 2023 года

# Отстройка **Netlas.io** от конкурентов. Инновации

- ✓ Больше чем пассивный сетевой сканер

**Netlas** предлагает множество дополнительных технических данных и специализированных инструментов, что существенно расширяет область его применения.

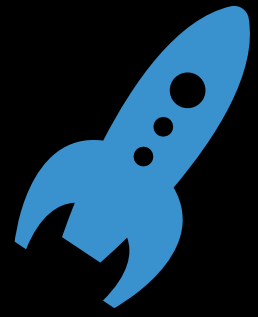
- ✓ Автоматизированное построение поверхности атаки

Функция, которая существенно снижает требования к квалификации пользователя, делая сервис доступнее и функциональнее.

- ✓ Мониторинг изменений поверхности атаки

Мониторинг не только заданного периметра, но и выявление новых объектов, относящихся к организации

# Состояние разработки



Январь 2021

## Создание прототипа

Май 2021

Проработка концепции проекта, разработка сканеров и баз данных, закупка специализированных серверов, предварительные сканы, сбор данных, разработка первой версии приложения Netlas, сайта-визитки.

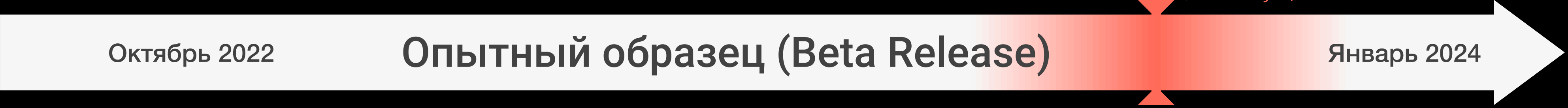


Октябрь 2022

## Стадия MVP (Alpha Release)

Май 2021

Публичное пилотирование, сбор обратной связи, участие в акселераторе, доработка концепции, сайта, доработка основных функций, интеграция с платежным сервисом.



Октябрь 2022

## Опытный образец (Beta Release)

Январь 2024

Появление платных акаунтов и функций (ограниченные бесплатные акаунты также остаются), улучшение качества, обеспечение отказоустойчивости, инструменты визуализации.

Текущий момент

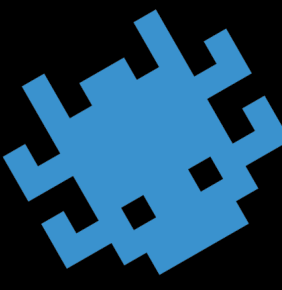


Июнь 2025

## Промышленный образец

Январь 2024

Совершенствование инструментов визуализации, разработка инструментов мониторинга, дополнительные функции, улучшающие и облегчающие работу с продуктом, оптимизация.



# Текущие успехи

~ 16,5 тыс.

Зарегистрированных  
пользователей

2x прирост за год

~ 12,5 тыс.

Ежемесячная аудитория сервиса  
(Monthly active users, **MAU**)

4x рост за год

до 700 тыс.

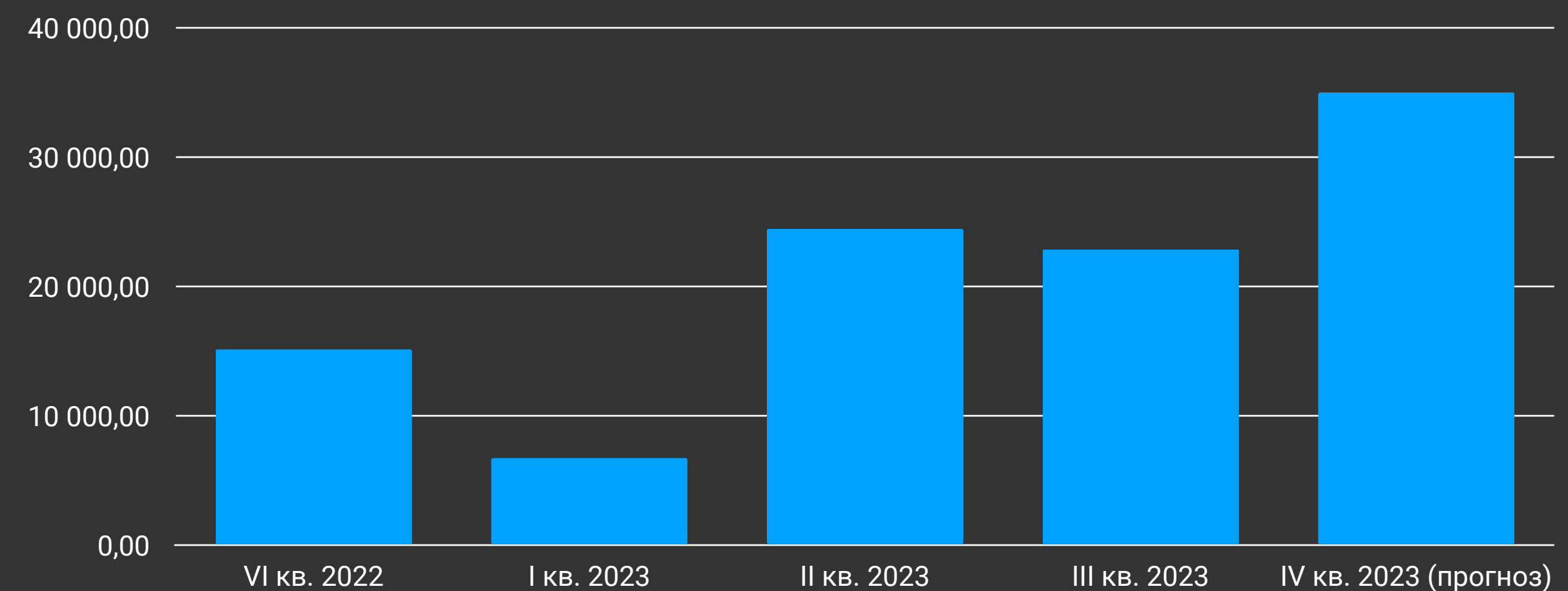
Запросов в месяц делают  
пользователи сервиса

**Netlas.io** – это web-сервис (SaaS модель).

Пользователи платят за:

- ✓ подписки для доступа, тарификация по количеству запросов, доступным данным и специальным функциям;
- ✓ единовременные покупки датасетов (представлены в магазине).

## Выручка от продаж через сайт, долл США



# Команда Netlas.io



**Артур Котылевский**

**Генеральный директор**

*17 лет опыта в управлении проектами.*

*9 лет опыта в управления предприятиями.*

*Профильное высшее образование  
(информационная безопасность).*

*2 патента в сфере информационной безопасности  
(автор).*



**Юрий Босов**

**Главный программист**

*12 лет опыта в сфере разработки программного  
обеспечения и информационной безопасности.*

*Профильное высшее образование  
(информационная безопасность).*

*Международный сертификат "Offensive Security  
Certified Professional".*

*Автор методики оценки устойчивости компании к  
методам взлома на основе социальной инженерии.*

Команда состоит из:

8

человек, включая разработчиков,  
тестировщиков, DevOps-специалиста и  
финансиста.

Разработка поддерживается:



Огромная благодарность фонду  
"Сколково" за менторскую и  
финансовую поддержку проекта, а  
также за предоставленные  
возможности по продвижению.



Огромная благодарность Фонду  
Бортника (ФСИ) за финансовую  
поддержку проекта.

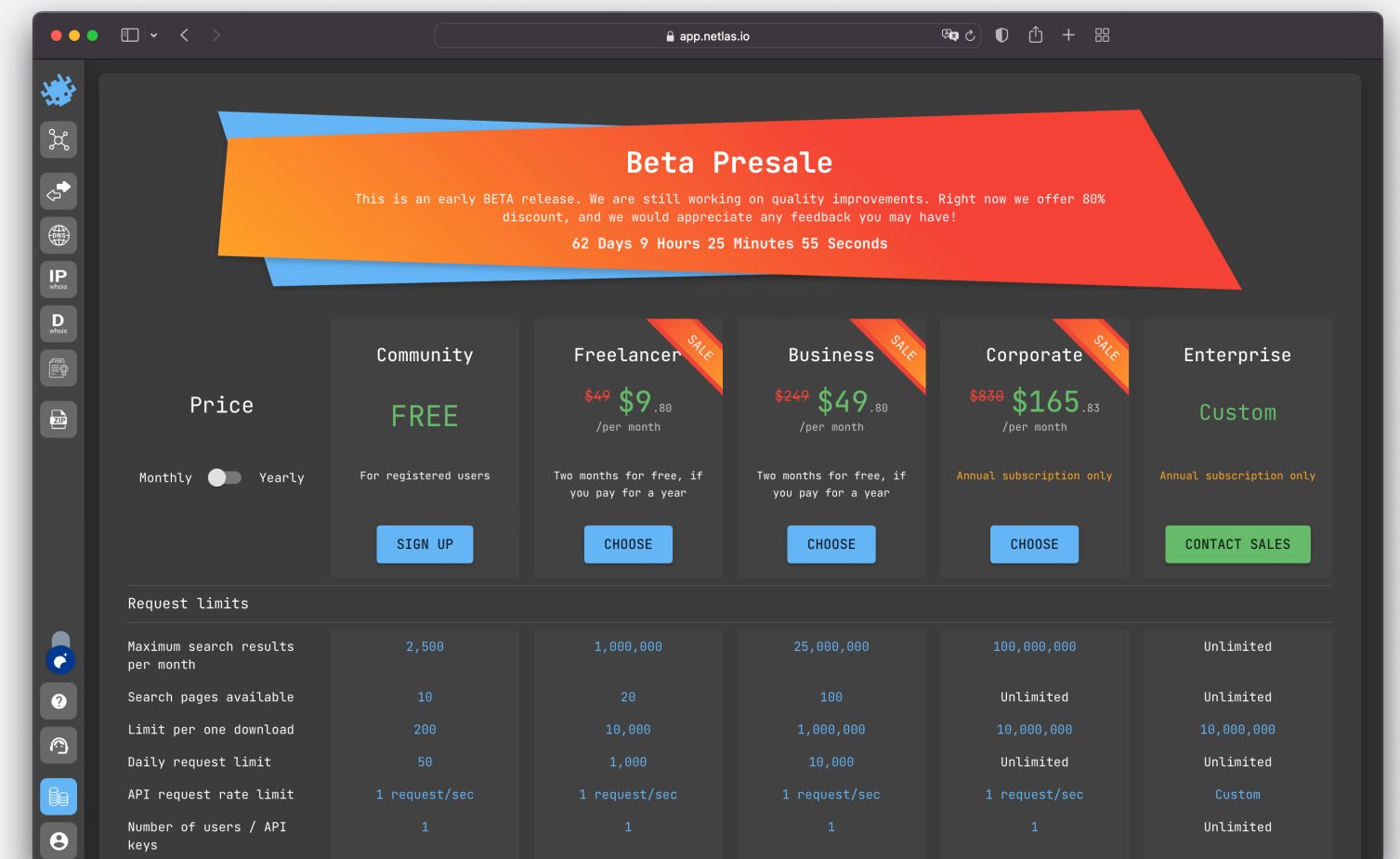
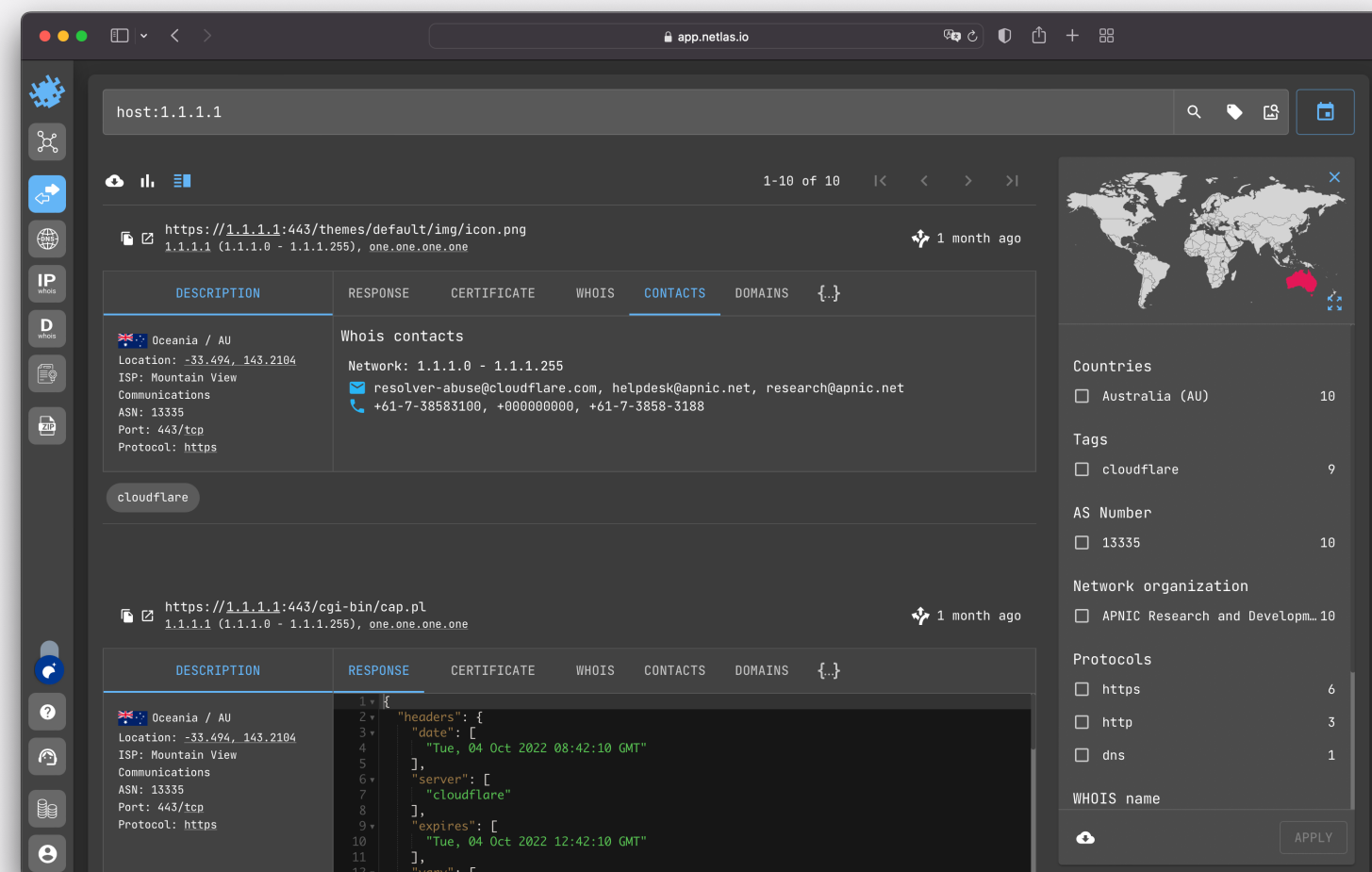
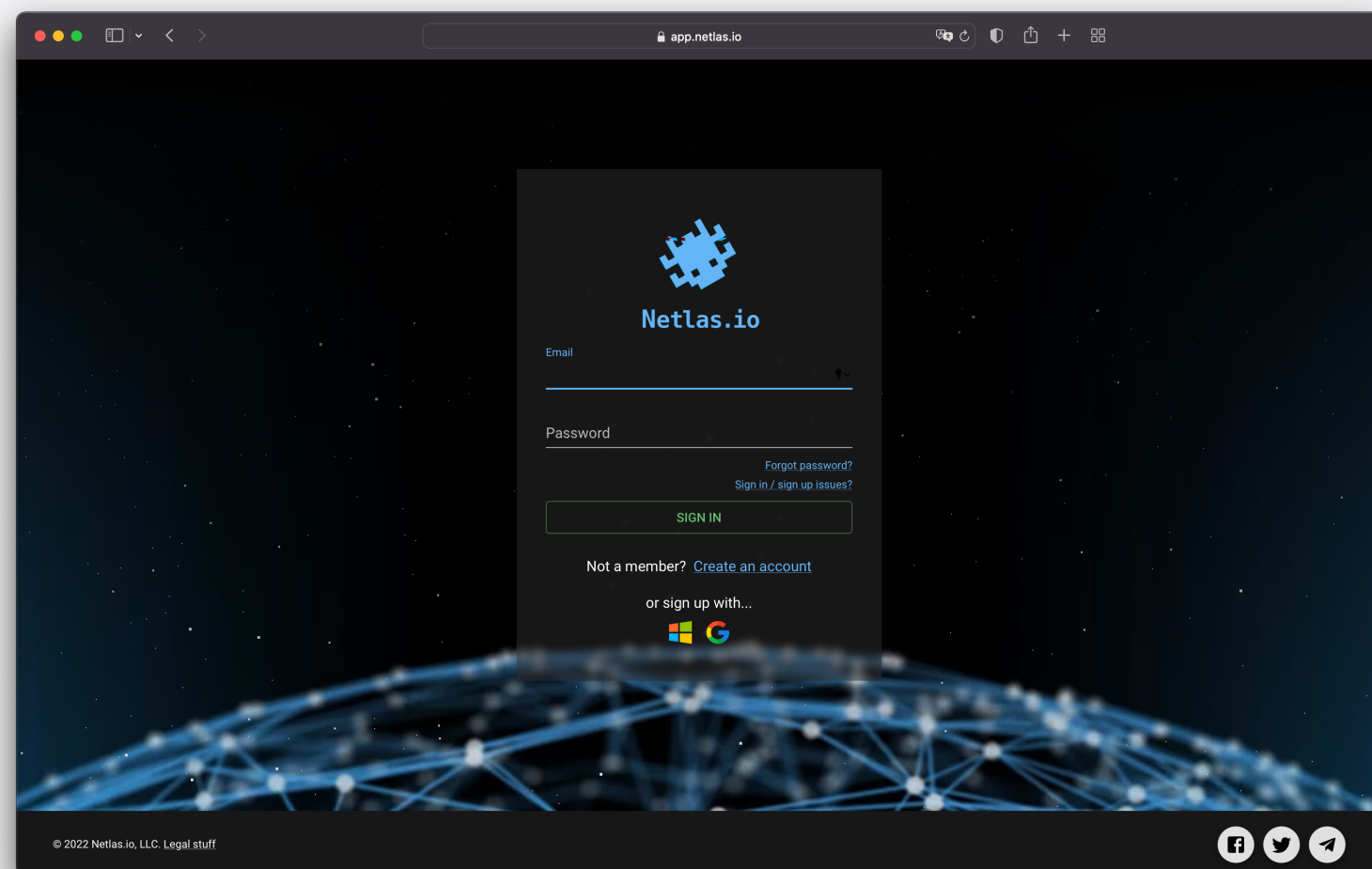
# Благодарю за внимание!

Артур Котылевский

Директор по развитию

+7 (921) 395-95-87

email: a.kotylevskiy@netlas.io



# Архитектура Netlas.io

