БЕЗОПАСНОСТЬ API ПРИЛОЖЕНИЙ В DEVOPS ПРОЦЕССАХ

ОБО МНЕ

- Развитие практик безопасной разработки приложений (AppSec)
- Исследование инструментов безопасности и уязвимостей
- Разработка и внедрение инструментов и процессов безопасности

Виталий Панасенко

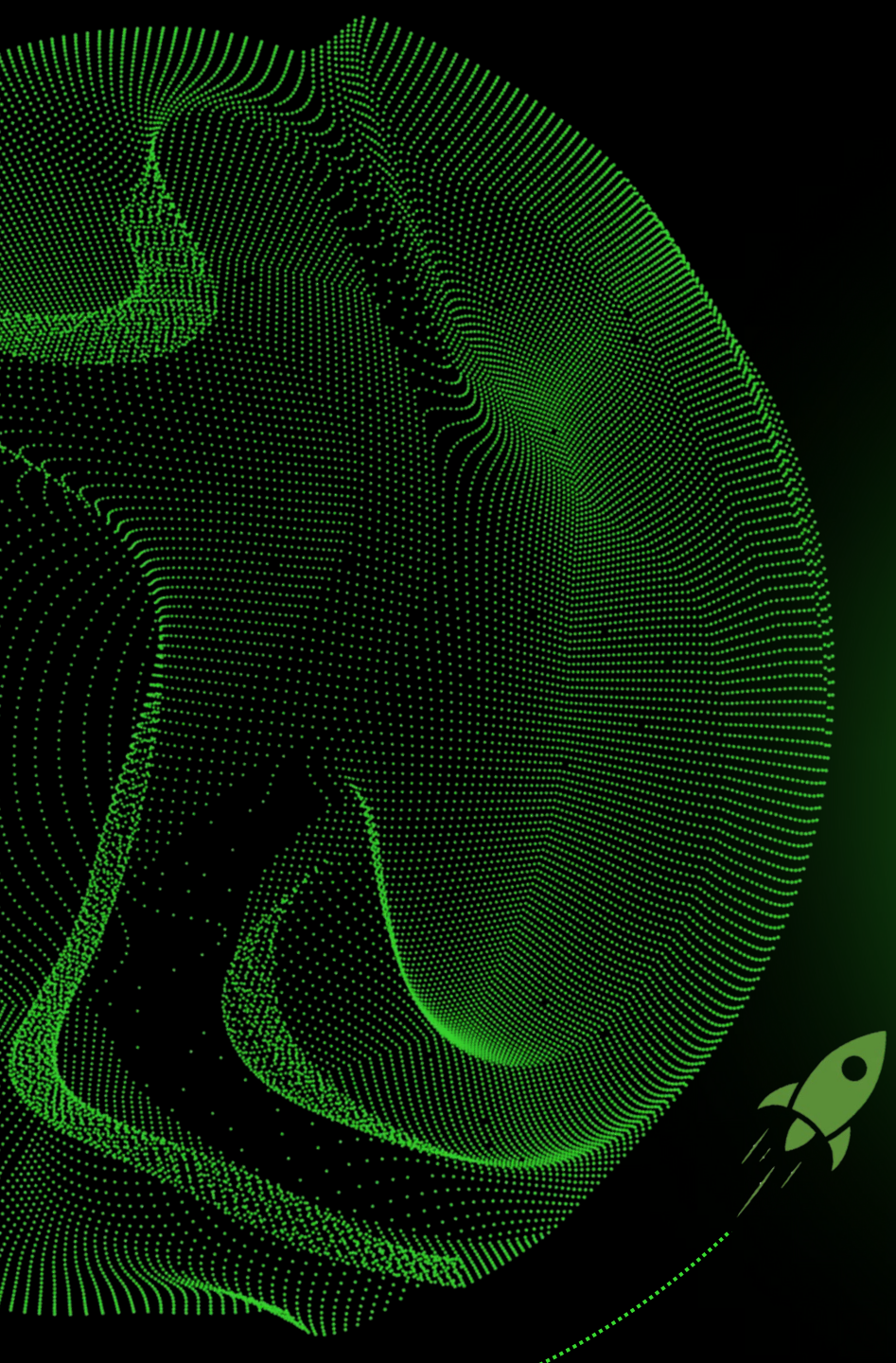
Независимый исследователь
Chief Product Officer, Москва

О НАС

OPEN SOURCE НЕ ПОМОГ

НАШ КЛИЕНТ И РЕШЕНИЕ

СТРАТЕГИИ



ARTIFICAL INTELLEGENCE

FOOD TECH

CYBERSECURITY

CLOUD SERVICES

BIOMETRY

50+
КОМПАНИЙ

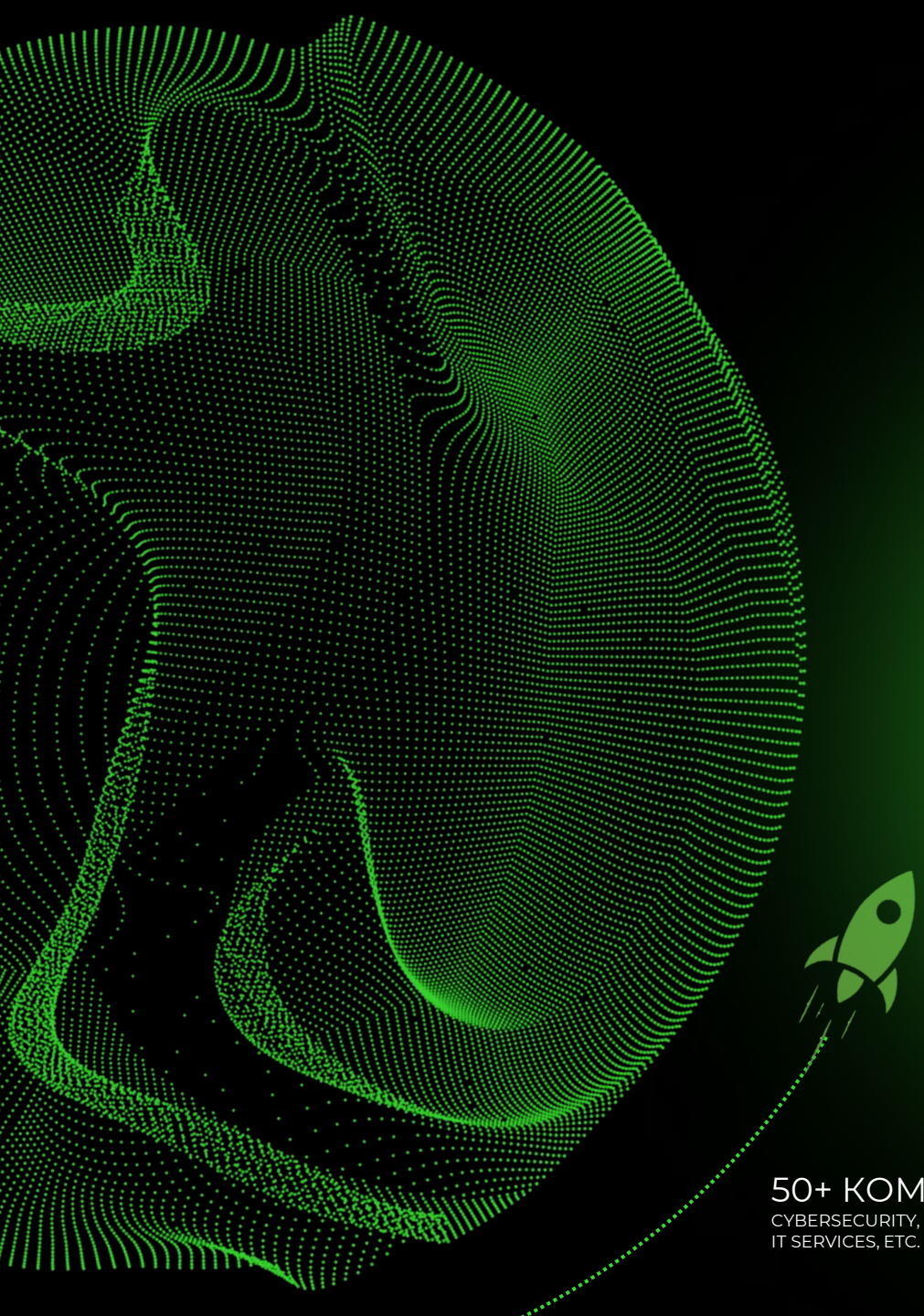
PROFESSIONAL SERVICES

FINANCIAL SERVICES

MARKTECH

IT SERVICES

ROBOTICS



МАШИНЫ

КОЛОНКИ

ТЕЛЕФОНЫ

ТЕЛЕВИЗОРЫ

1000+
ПРИЛОЖЕНИЙ

КОМПЬЮТЕРЫ

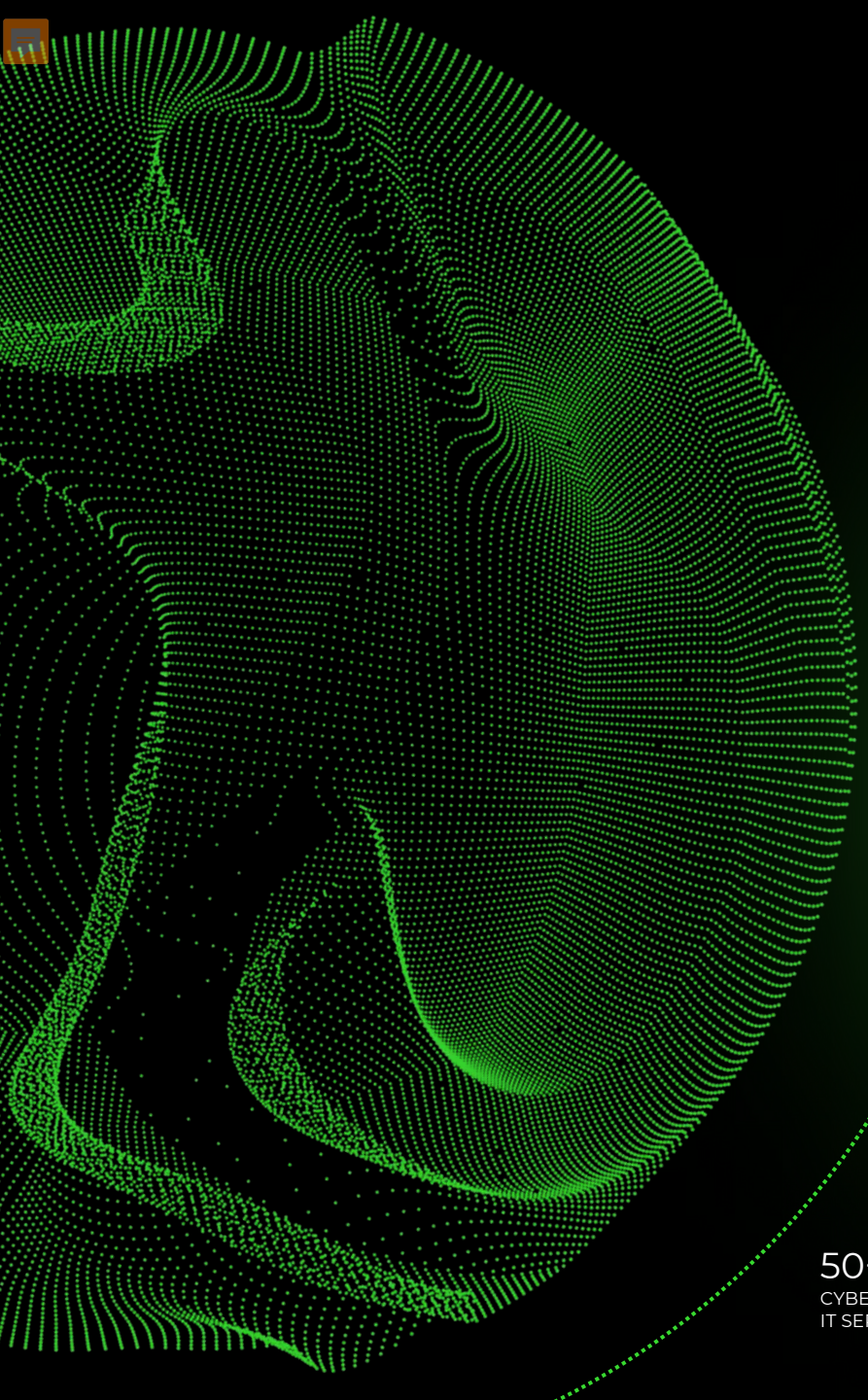
КОМПЬЮТЕРЫ

РОБОТЫ

ОПЕРАЦИОННАЯ СИСТЕМА

50+ КОМПАНИЙ

CYBERSECURITY, BIOMETRY,
IT SERVICES, ETC.

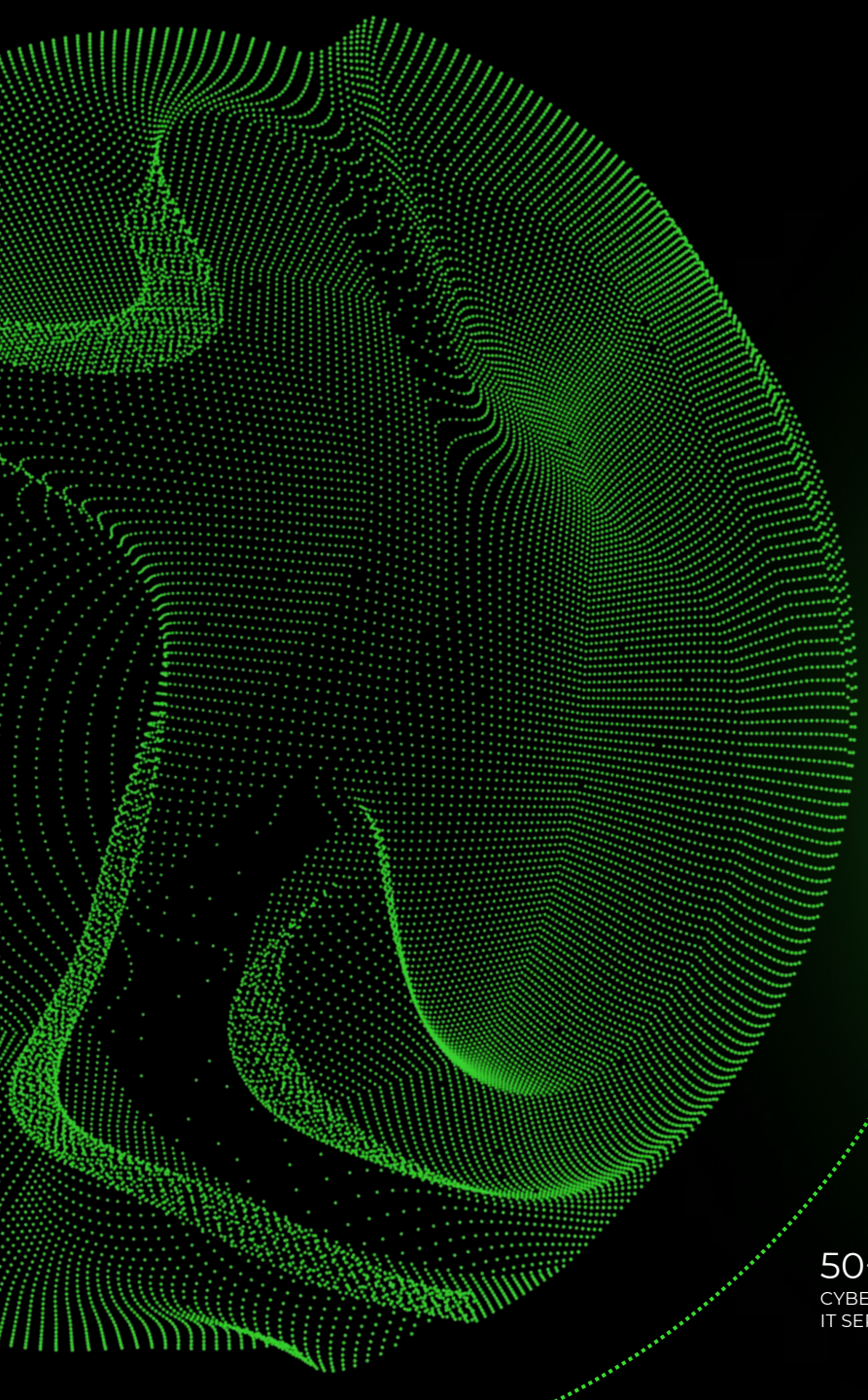


1000+ APPS
MOBILE, WEB, ROBOTS,
AI, OS & ETC.

50+ КОМПАНИЙ
CYBERSECURITY, BIOMETRY,
IT SERVICES, ETC.

100+

ЯЗЫКОВ ПРОГРАММИРОВАНИЯ



100+ ЯП

JAVA, GO, PYTHON,
JS, C++ & ETC.

1000+ APPS

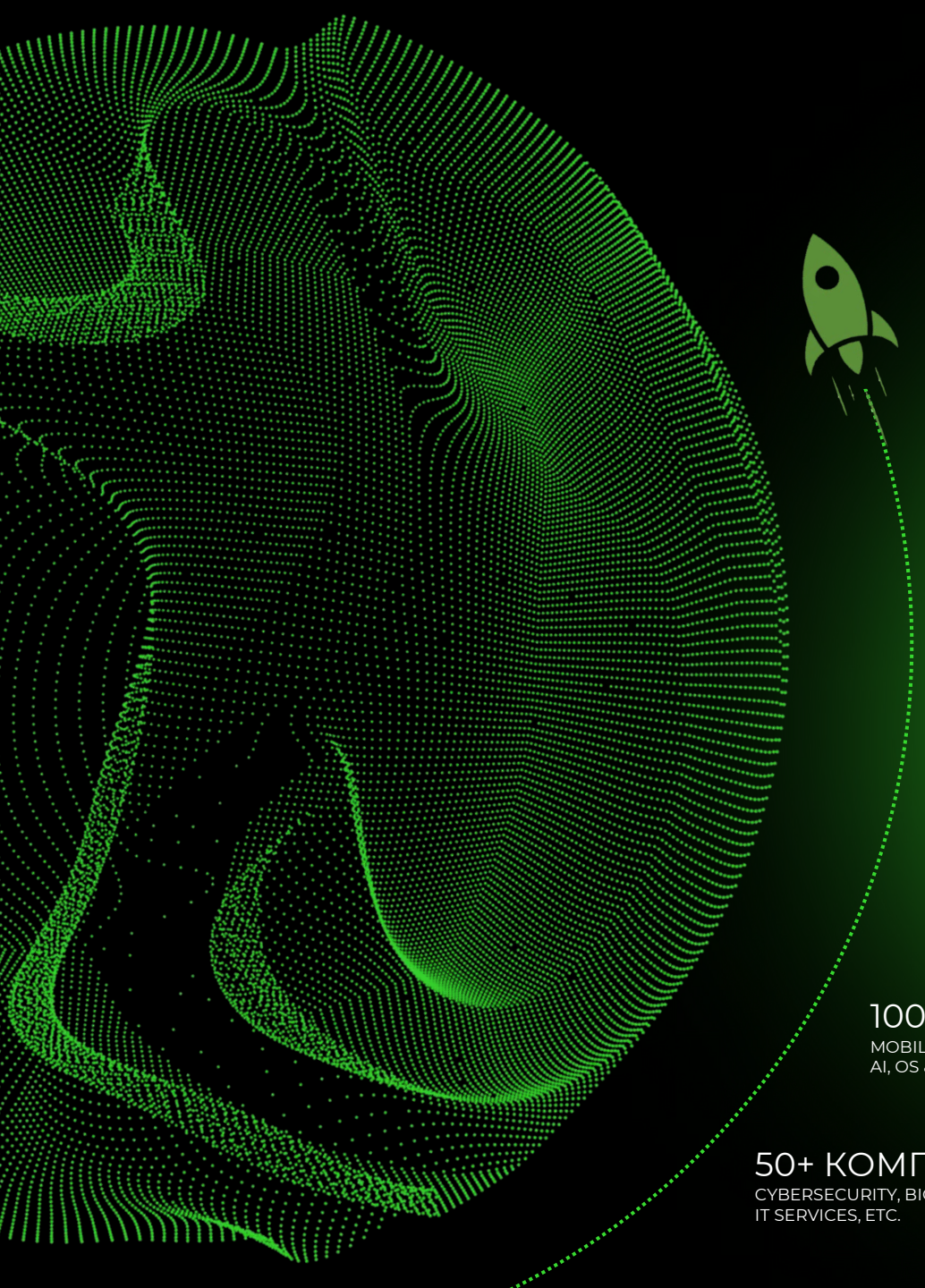
MOBILE, WEB, ROBOTS,
AI, OS & ETC.

50+ КОМПАНИЙ

CYBERSECURITY, BIOMETRY,
IT SERVICES, ETC.

5000+

КОМАНД



5000+
AGILE КОМАНД.

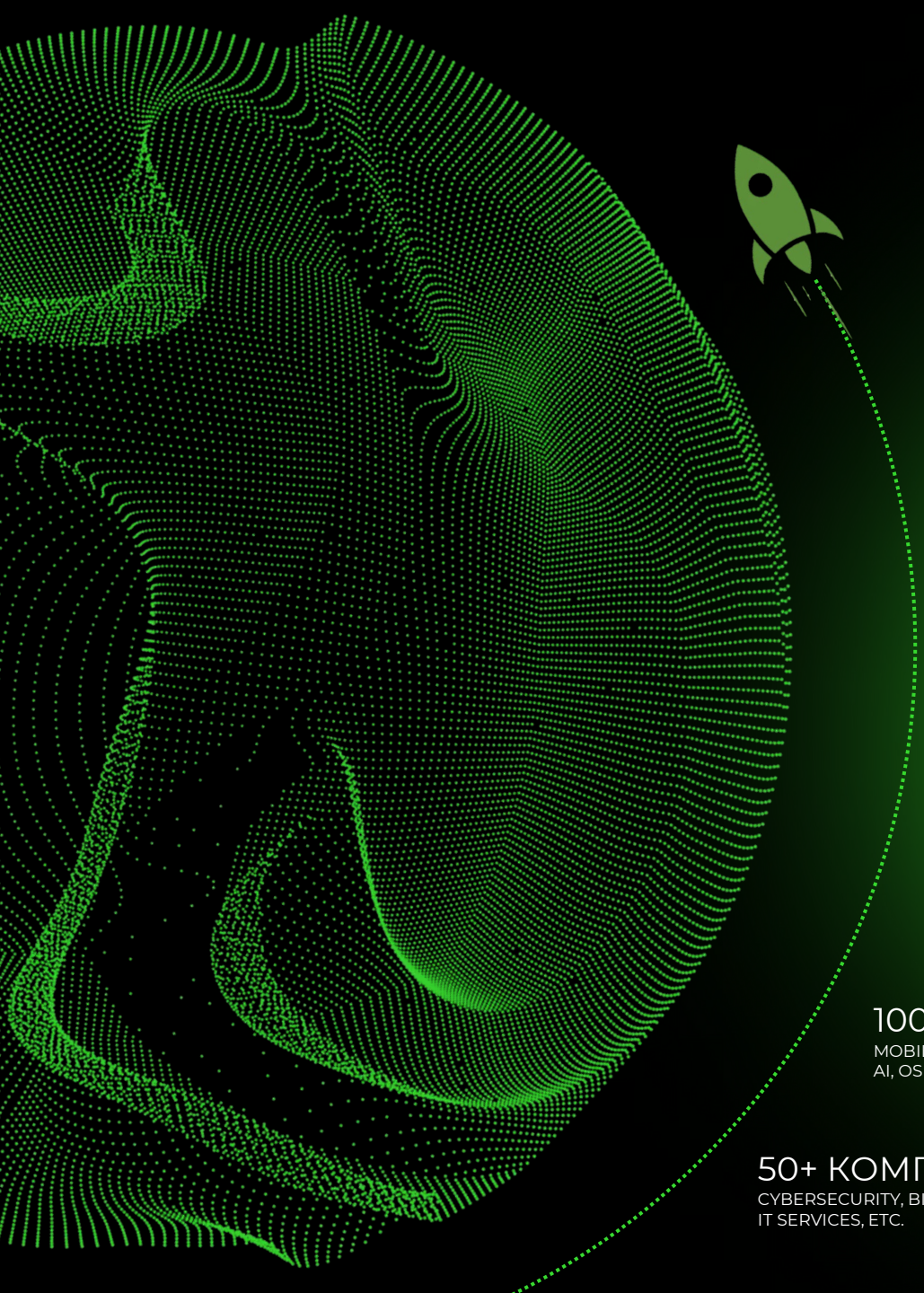
100+ ЯП
JAVA, GO, PYTHON,
JS, C++ & ETC.

1000+ APPS
MOBILE, WEB, ROBOTS,
AI, OS & ETC.

50+ КОМПАНИЙ
CYBERSECURITY, BIOMETRY,
IT SERVICES, ETC.

7 ДНЕЙ

TIME TO MERKET



7 ДНЕЙ
TIME TO MARKET

5000+
AGILE КОМАНД.

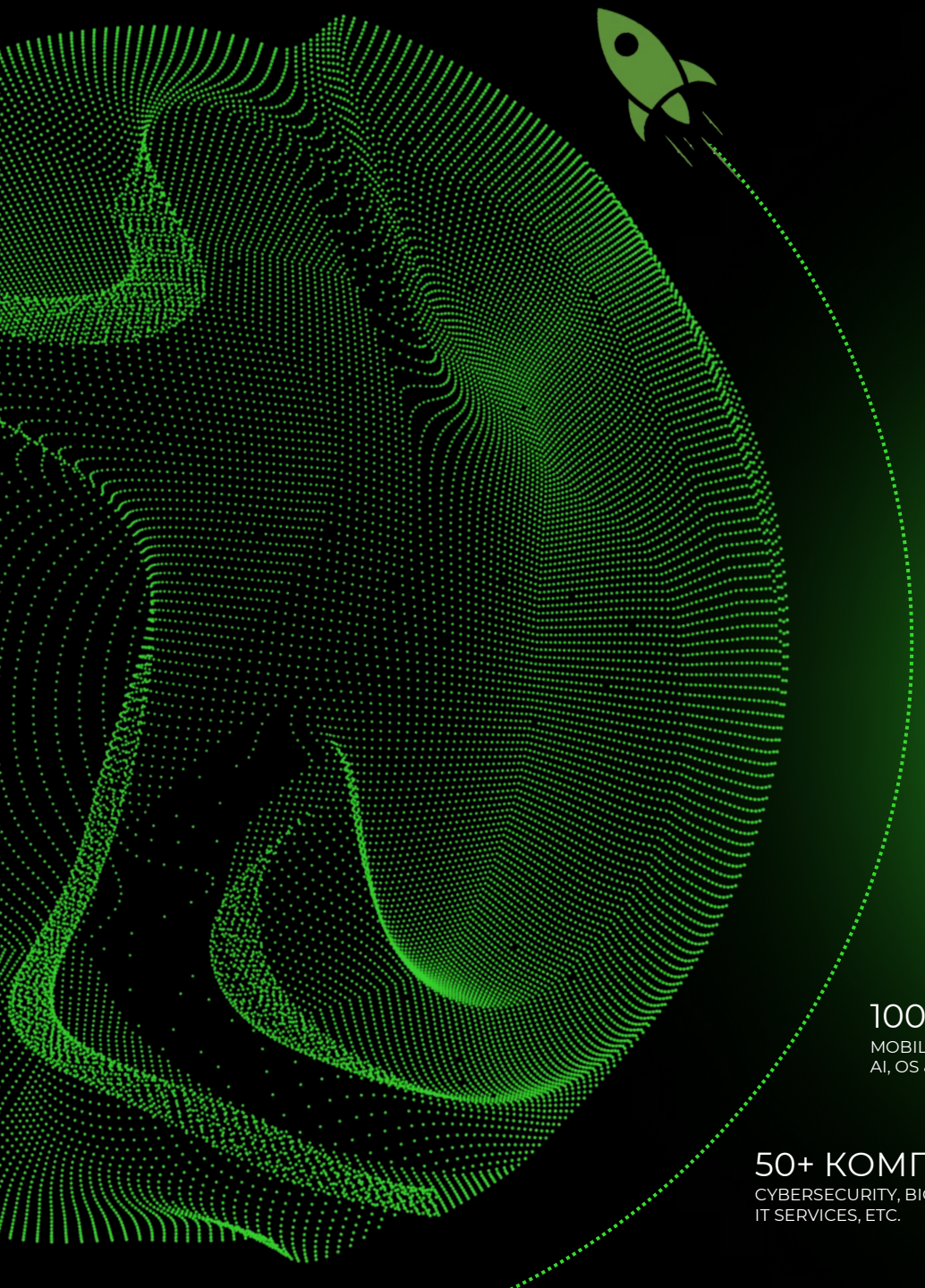
100+ ЯП
JAVA, GO, PYTHON,
JS, C++ & ETC.

1000+ APPS
MOBILE, WEB, ROBOTS,
AI, OS & ETC.

50+ КОМПАНИЙ
CYBERSECURITY, BIOMETRY,
IT SERVICES, ETC.

100 МЛН.

КЛИЕНТОВ



100 МЛН.
КЛИЕНТОВ

7 ДНЕЙ
TIME TO MARKET

5000+
AGILE КОМАНД.

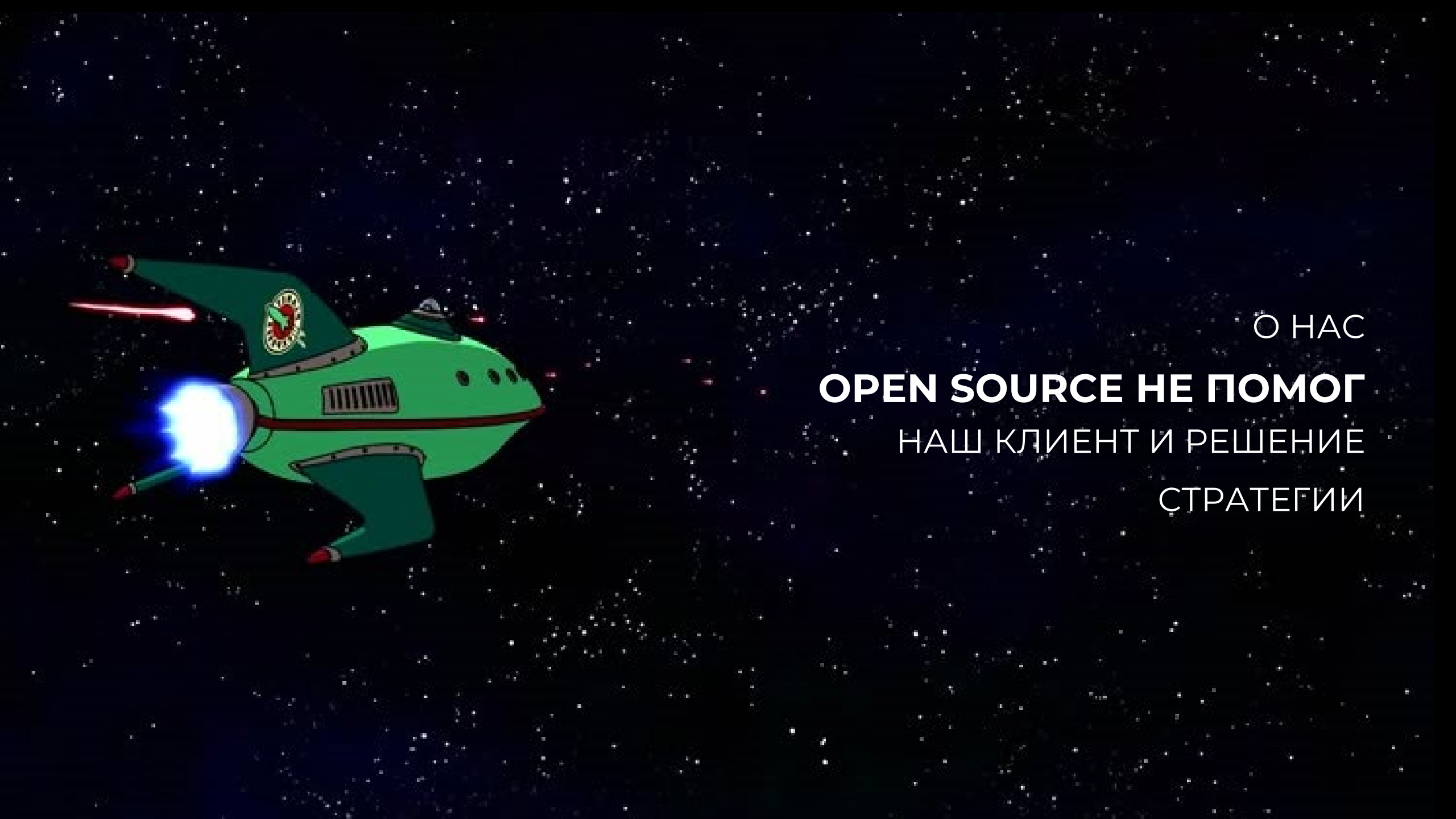
100+ ЯП
JAVA, GO, PYTHON,
JS, C++ & ETC.

1000+ APPS
MOBILE, WEB, ROBOTS,
AI, OS & ETC.

50+ КОМПАНИЙ
CYBERSECURITY, BIOMETRY,
IT SERVICES, ETC.

1.9 ТРЛН.

РУБЛЕЙ



О НАС

OPEN SOURCE НЕ ПОМОГ

НАШ КЛИЕНТ И РЕШЕНИЕ

СТРАТЕГИИ

ЧТО ТАКОЕ APIFUZZING?

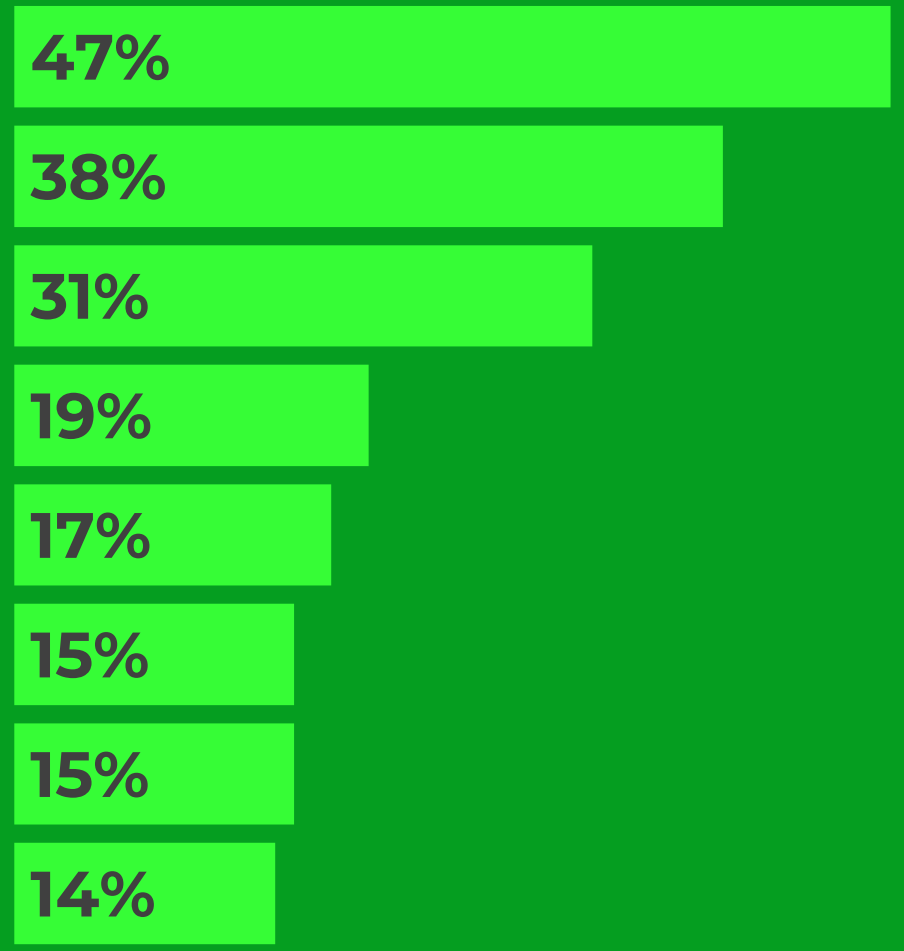
Это метод, используемый для проверки безопасности и надежности API приложений. Fuzzing подразумевает **отправку** большого количества **некорректных** или **неожиданных** входных **данных в API для выявления** потенциальных **уязвимостей**, таких как проблемы проверки входных данных, переполнения буфера, инъекционные атаки или другие типы уязвимостей безопасности.

ЧТО В МИРЕ?

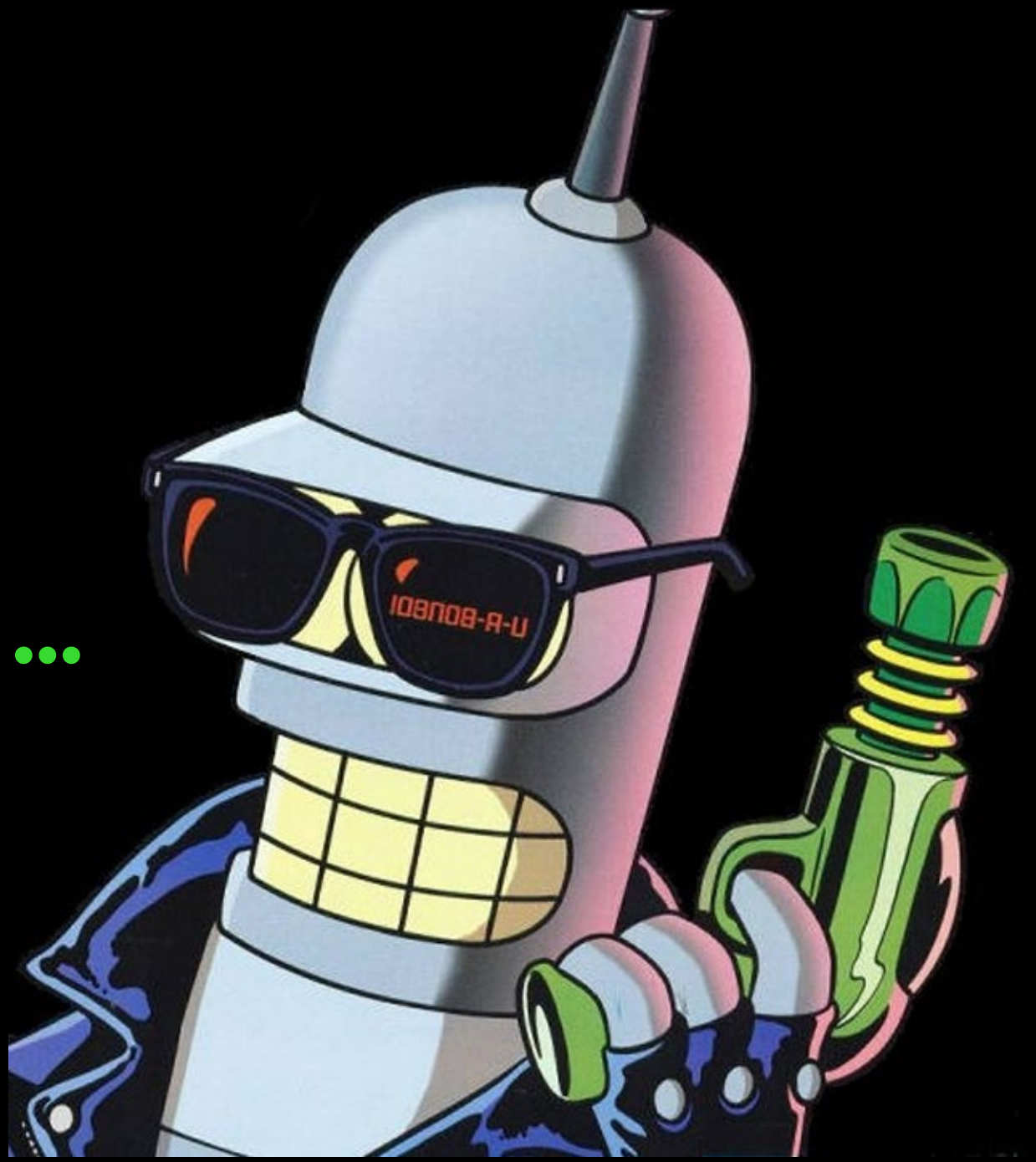
КОМПАНИЙ СТАЛКИВАЛИСЬ С ПРОБЛЕМАМИ **94%**

11% КОМПАНИЙ РЕАЛИЗУЮТ СТРАТЕГИИ ЗАЩИТЫ

ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ В API



МЫ РЕШИЛИ,
ЧТО САМЫЕ УМНЫЕ ...



ЧТО ЕСТЬ НА РЫНКЕ?

- Анализ схем OpenAPI/GraphQL
- Мутационная генерация проверок
- Проверка в многопоточности
- Наличие CVE-словарей

ИНСТРУМЕНТ	ПОКРЫТИЕ	ТОЧНОСТЬ	ТЕХНОЛОГ.	SDLC	УДОБСТВО
CATS	★	★	★	★★	★
Ffuf	★	★	★	★★	★
Wfuzz	★	★	★	★★	★
API-Fuzzer	★	★	★	★★	★
Restler	★	★	★	★★	★

ВЫБРАЛИ WFUZZ

- **ПРОСТОЙ** Python ФАЙЗЕР
- ОДИН ИЗ САМЫХ **ПОПУЛЯРНЫХ** ФАЙЗЕРОВ
- **ВЫСОКИЕ ОЦЕНКИ** НА GITHUB (6.1k звезд)
- **ЧАСТЫ ОБНОВЛЕНИЕ** СО СТОРОНЫ СООБЩЕСТА

ПОТЕРПЕЛИ
НЕУДАЧУ

О НАС

OPEN SOURCE НЕ ПОМОГ

НАШ КЛИЕНТ И РЕШЕНИЕ

СТРАТЕГИИ

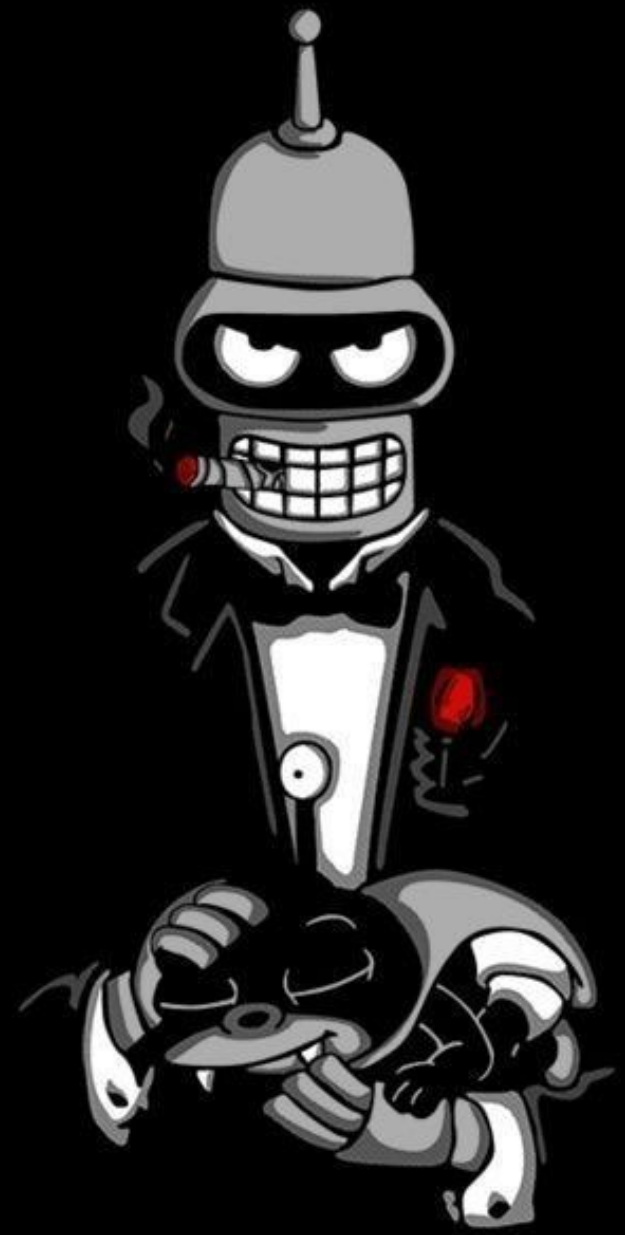
НУЖЕН ЛИ
КЛИЕНТАМ APIFUZZING?

СЧИТАЮТ ВАЖНЫМ ПРОВЕРКИ **90%**

94% ХОТЯТ ПРОВЕРКИ В CI/CD

ЧТО ТРЕБУЕТСЯ **КЛИЕНТАМ?**

- Максимально **простые проверки** на сколько это возможно
- Максимально **точное обнаружение** проблем в API
- **Широкое покрытие** технологий для проверки систем
- **Минимальное время** на проверку **и минимальные знания** в области КБ
- Инструмент должен уметь **работать с авторизацией**



ПРОСТОЕ ПОДКЛЮЧЕНИЕ И ЗАПУСК ПРОВЕРКИ

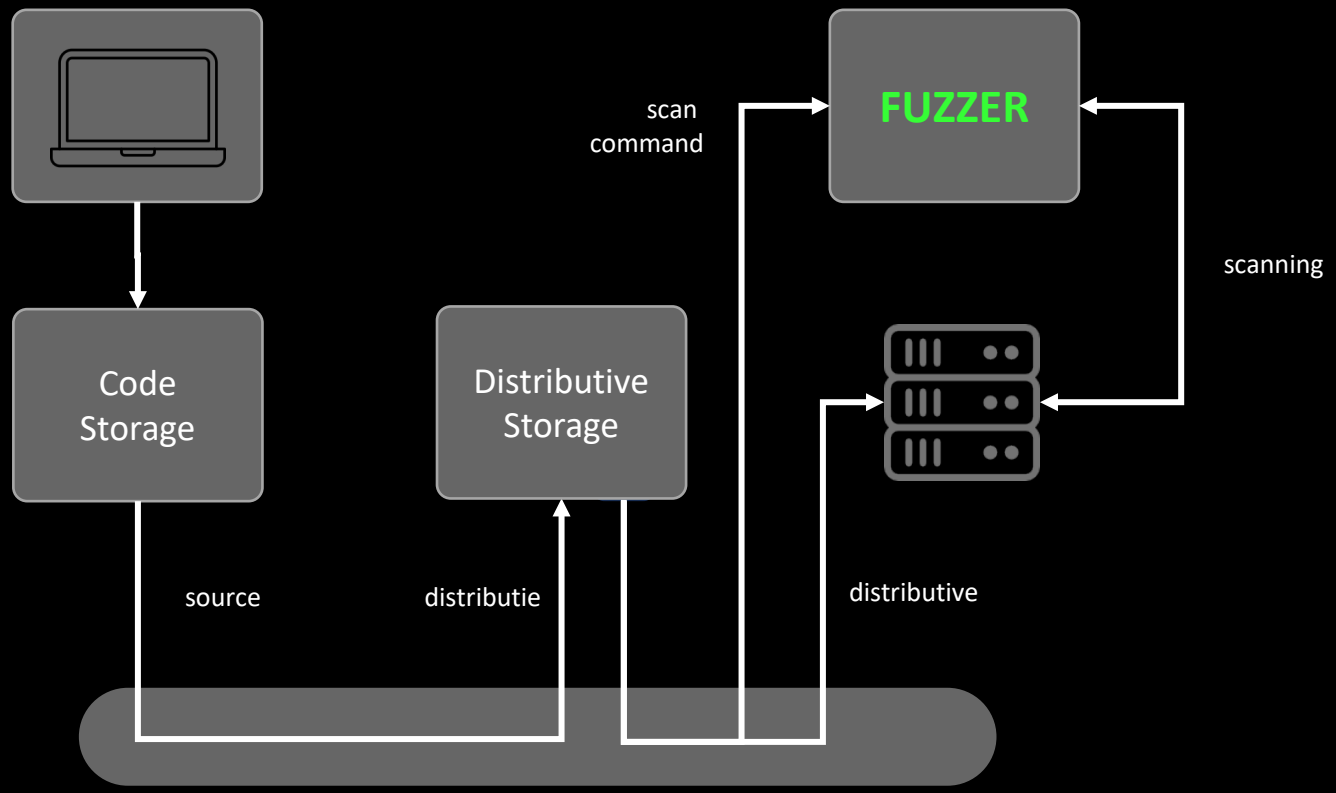
ВЫСОКАЯ ТОЧНОСТЬ ОБНАРУЖЕНИЯ

ШИРОКОЕ ПОКРЫТИЕ ПРОВЕРЯЕМЫХ ТЕХНОЛОГ.

МИНИМАЛЬНОЕ ВРЕМЯ НА ПРОВЕРКУ

МИНИМАЛЬНЫЕ ЗНАНИЯ В ОБЛАСТИ КБ

АВТОМАТИЗИРУЙТЕ ПРОВЕРКИ В CI/CD



ПРОСТОЕ ПОДКЛЮЧЕНИЕ И ЗАПУСК ПРОВЕРКИ

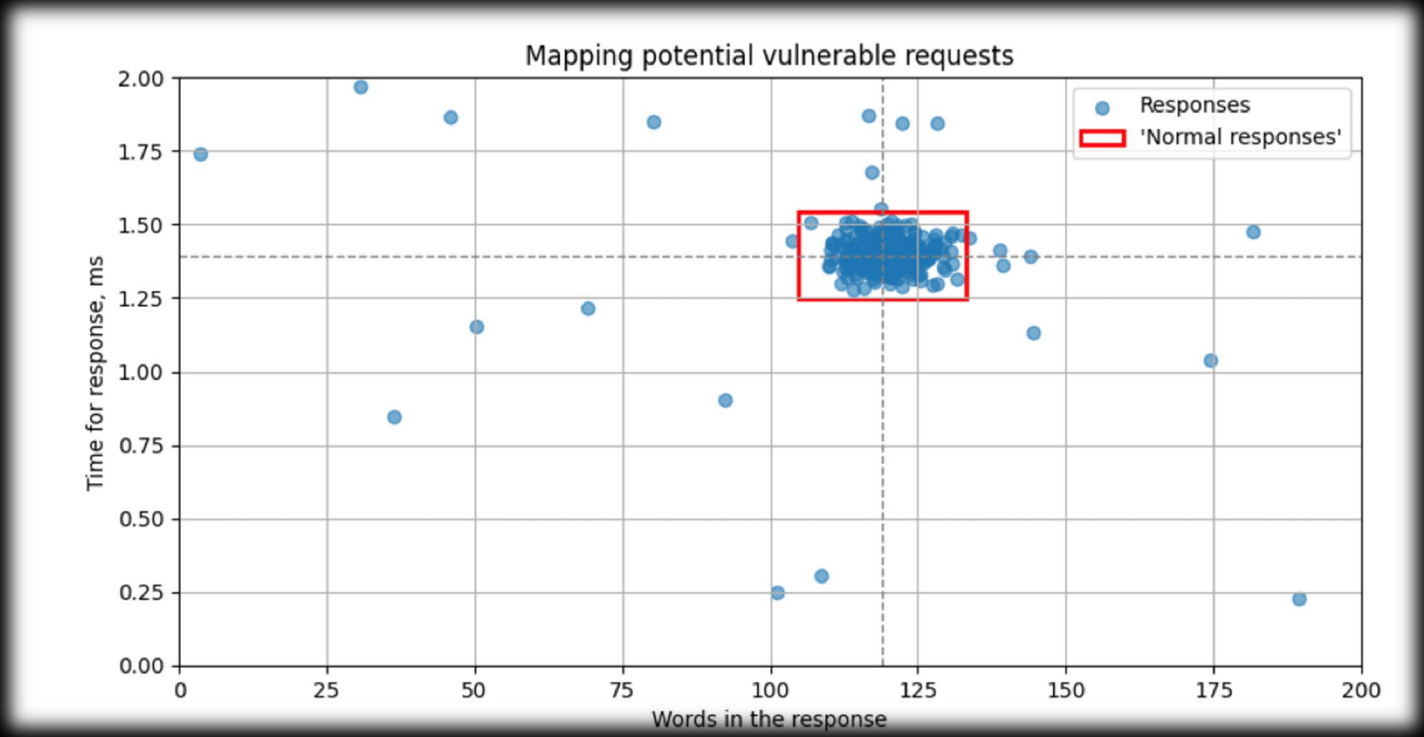
ВЫСОКАЯ ТОЧНОСТЬ ОБНАРУЖЕНИЯ

ШИРОКОЕ ПОКРЫТИЕ ПРОВЕРЯЕМЫХ ТЕХНОЛОГ.

МИНИМАЛЬНОЕ ВРЕМЯ НА ПРОВЕРКУ

МИНИМАЛЬНЫЕ ЗНАНИЯ В ОБЛАСТИ КБ

СОСРЕДОТОЧТЕСЬ НА ДЕЙСТВИТЕЛЬНО ВАЖНОМ



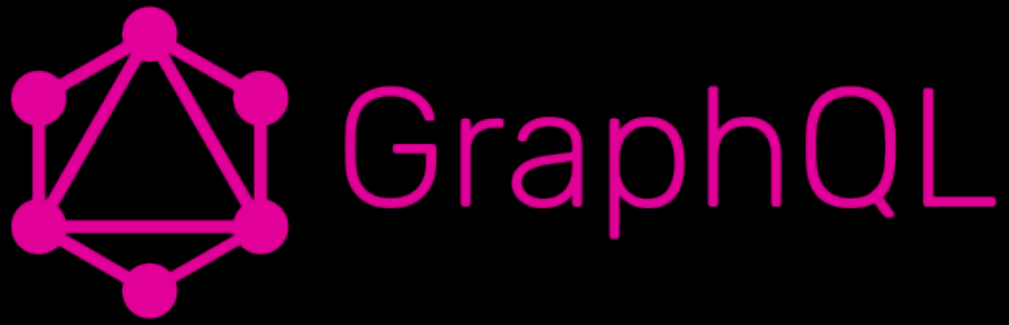
ПРОСТОЕ ПОДКЛЮЧЕНИЕ И ЗАПУСК ПРОВЕРКИ

ВЫСОКАЯ ТОЧНОСТЬ ОБНАРУЖЕНИЯ

ШИРОКОЕ ПОКРЫТИЕ ПРОВЕРЯЕМЫХ ТЕХНОЛОГ.

МИНИМАЛЬНОЕ ВРЕМЯ НА ПРОВЕРКУ

МИНИМАЛЬНЫЕ ЗНАНИЯ В ОБЛАСТИ КБ



ПРОСТОЕ ПОДКЛЮЧЕНИЕ И ЗАПУСК ПРОВЕРКИ

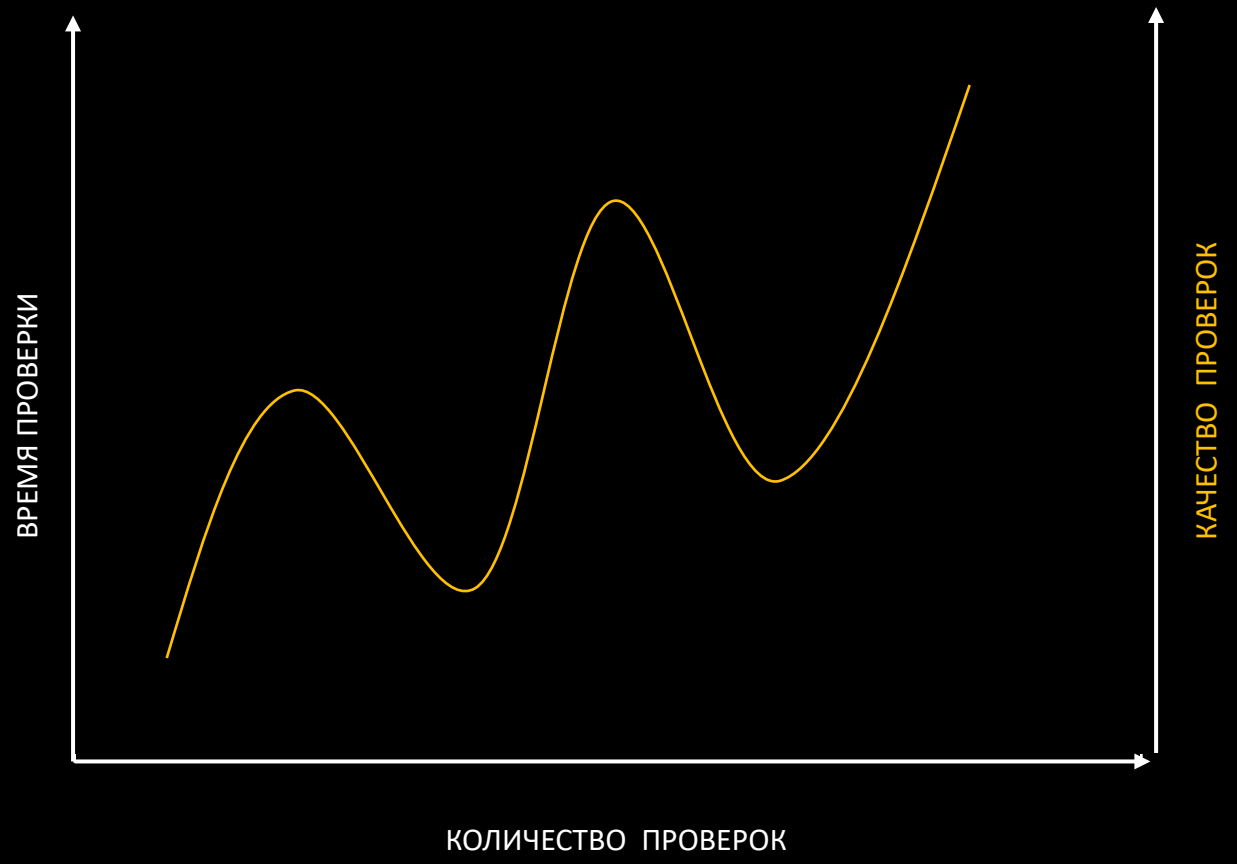
ВЫСОКАЯ ТОЧНОСТЬ ОБНАРУЖЕНИЯ

ШИРОКОЕ ПОКРЫТИЕ ПРОВЕРЯЕМЫХ ТЕХНОЛОГ.

МИНИМАЛЬНОЕ ВРЕМЯ НА ПРОВЕРКУ

МИНИМАЛЬНЫЕ ЗНАНИЯ В ОБЛАСТИ КБ

ВЫБИРАЙТЕ ОПТИМАЛЬНЫЙ РЕЖИМ ПРОВЕРОК



ПРОСТОЕ ПОДКЛЮЧЕНИЕ И ЗАПУСК ПРОВЕРКИ

ВЫСОКАЯ ТОЧНОСТЬ ОБНАРУЖЕНИЯ

ШИРОКОЕ ПОКРЫТИЕ ПРОВЕРЯЕМЫХ ТЕХНОЛОГ.

МИНИМАЛЬНОЕ ВРЕМЯ НА ПРОВЕРКУ

МИНИМАЛЬНЫЕ ЗНАНИЯ В ОБЛАСТИ КБ

ОПРЕДЕЛИТЬ СЦЕНАРИИ ПРОВЕРОК

Module
Vuln Testing

Module
DoS &
DDoS

Module
Role
Testing

Module Fing
Hiden Endpoint

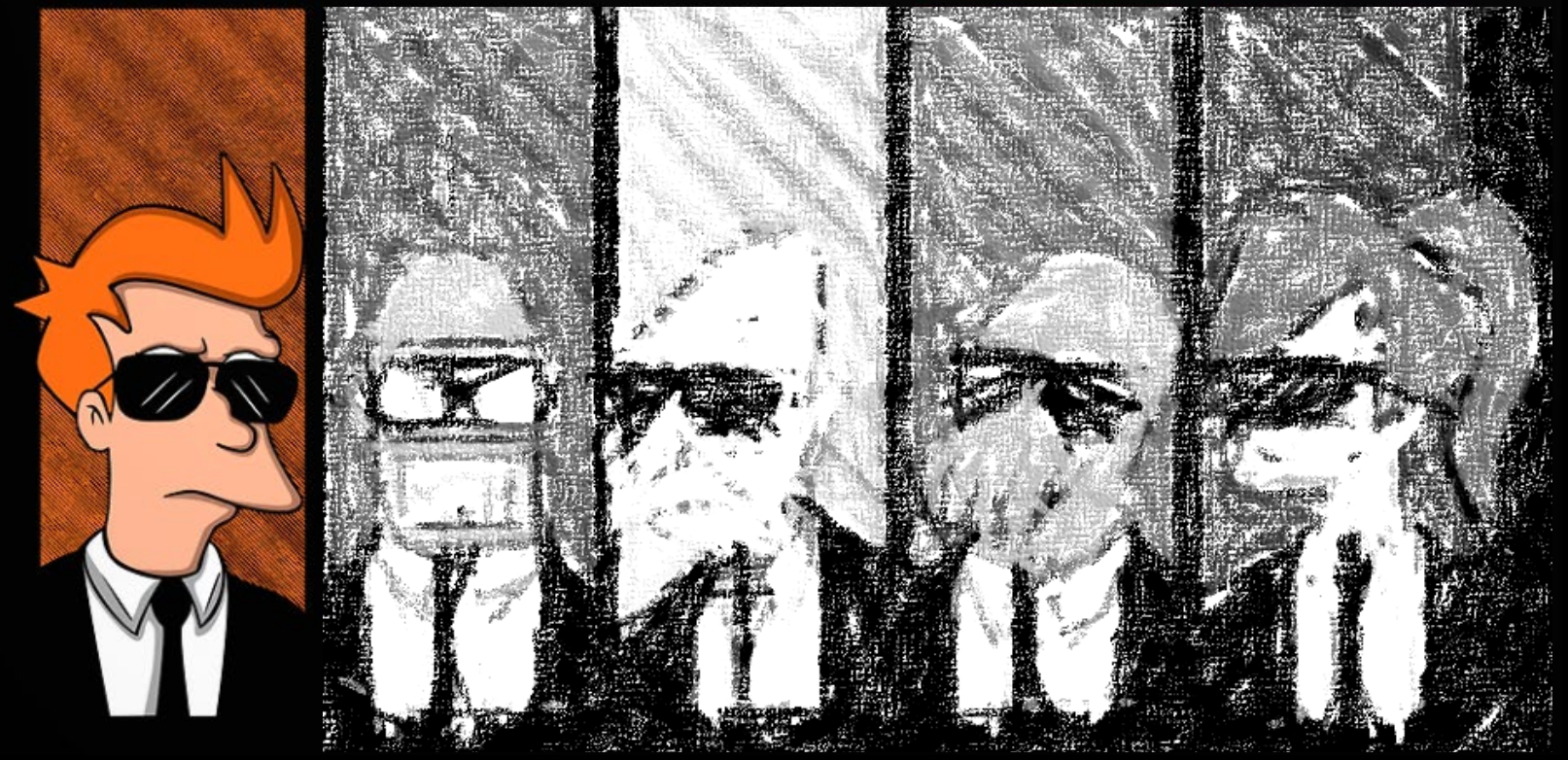
О НАС

OPEN SOURCE НЕ ПОМОГ

НАШ КЛИЕНТ И РЕШЕНИЕ

СТРАТЕГИИ

СТРАТЕГИИ ЗАЩИТЫ API



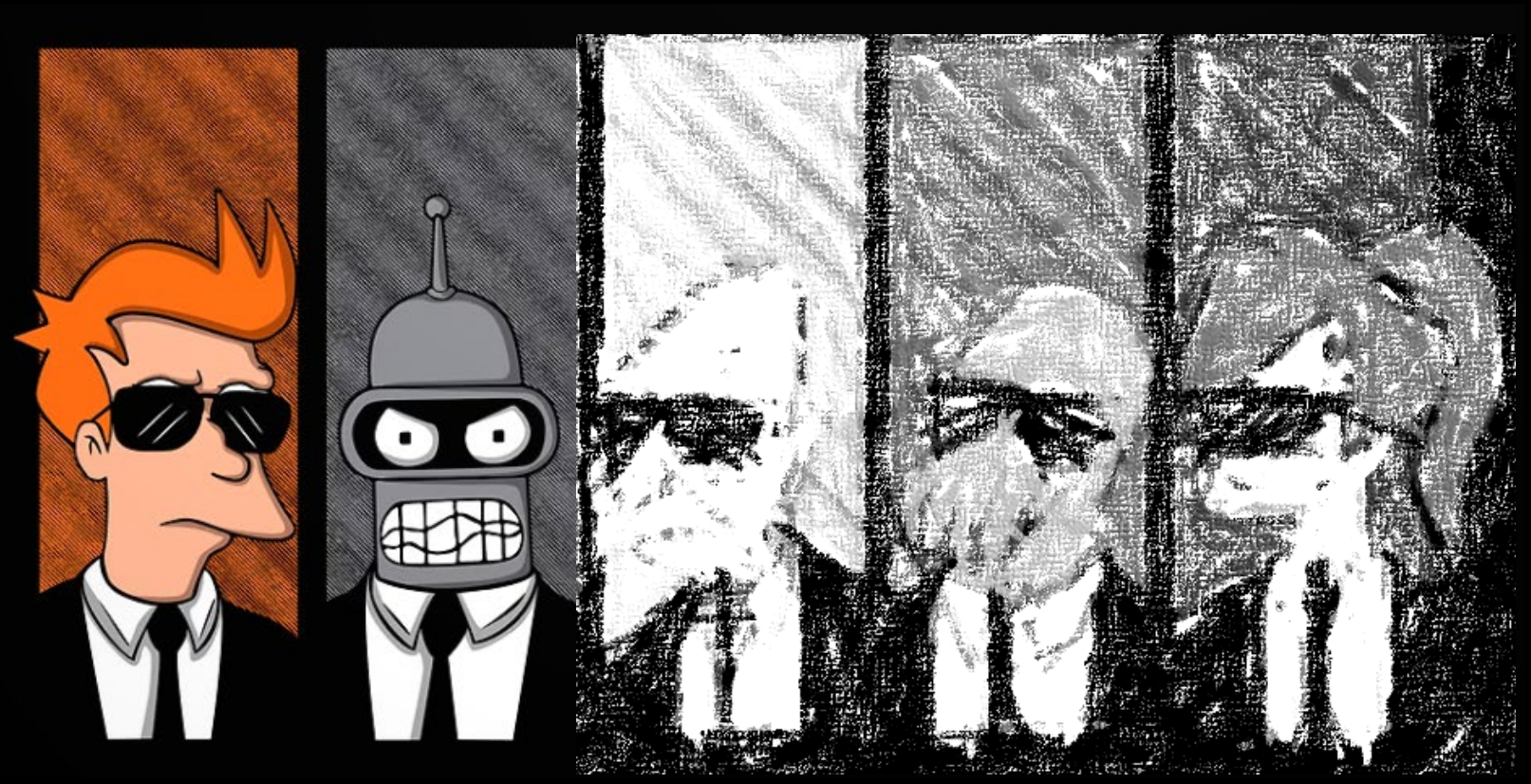
AuthN & AuthZ | Input Val. & Sanit. | HTTPS & Data Encrypt. | Rate Limit & unDoS | Monitoring & Audit

Аутентификация и авторизация

Используйте OAuth 2.0 с JWT-токенами и ролевую модель (RBAC)

Без этого даже самый крутой API уязвим для взлома

СТРАТЕГИИ ЗАЩИТЫ API



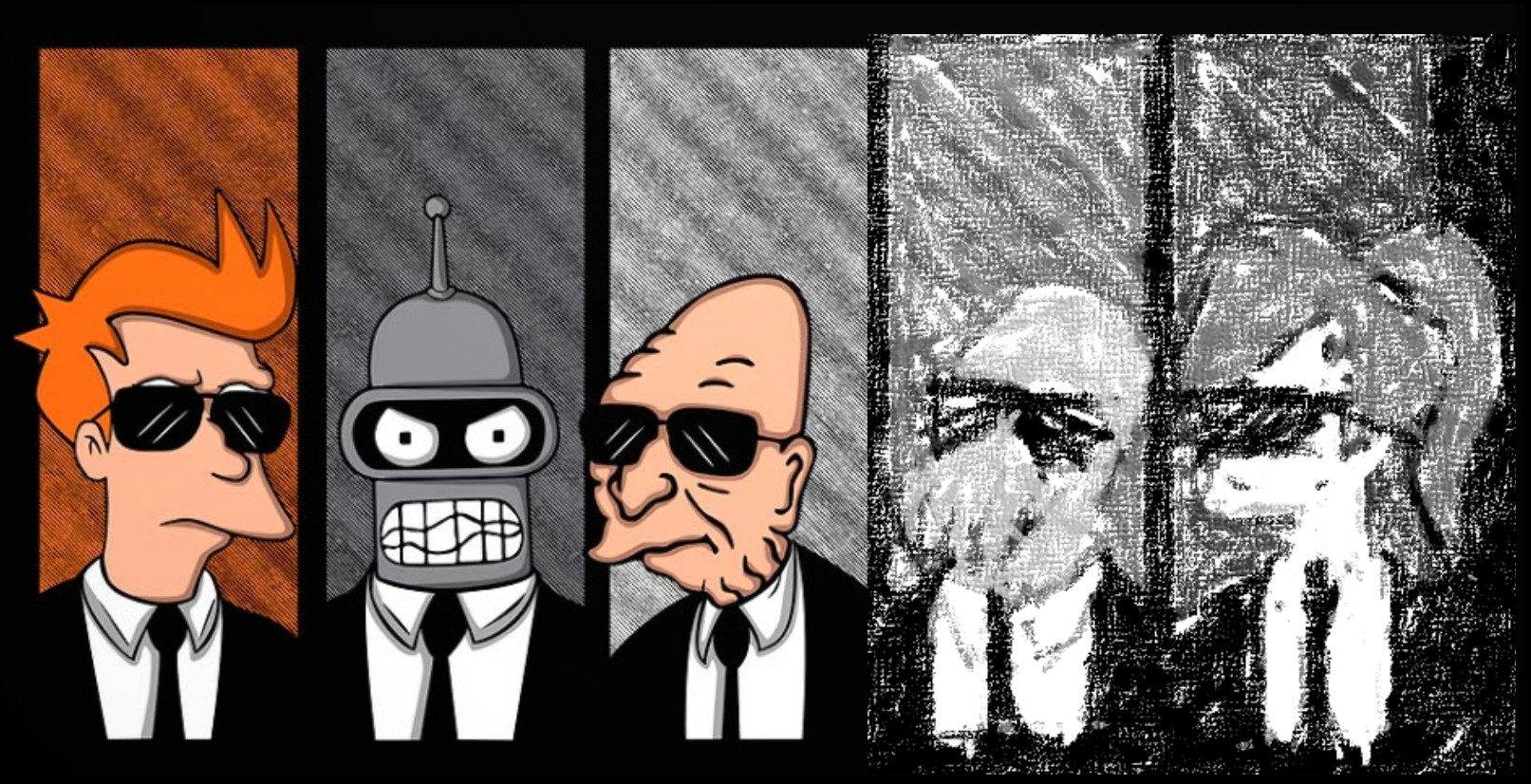
AuthN & AuthZ | Input Val. & Sanit. | HTTPS & Data Encrypt. | Rate Limit & unDoS | Monitoring & Audit

Валидация и санитизация данных

Проверяйте все параметры запросов и фильтруйте опасные символы (SQL-инъекции, XSS).

Даже одна уязвимость может привести к утечке данных

СТРАТЕГИИ ЗАЩИТЫ API



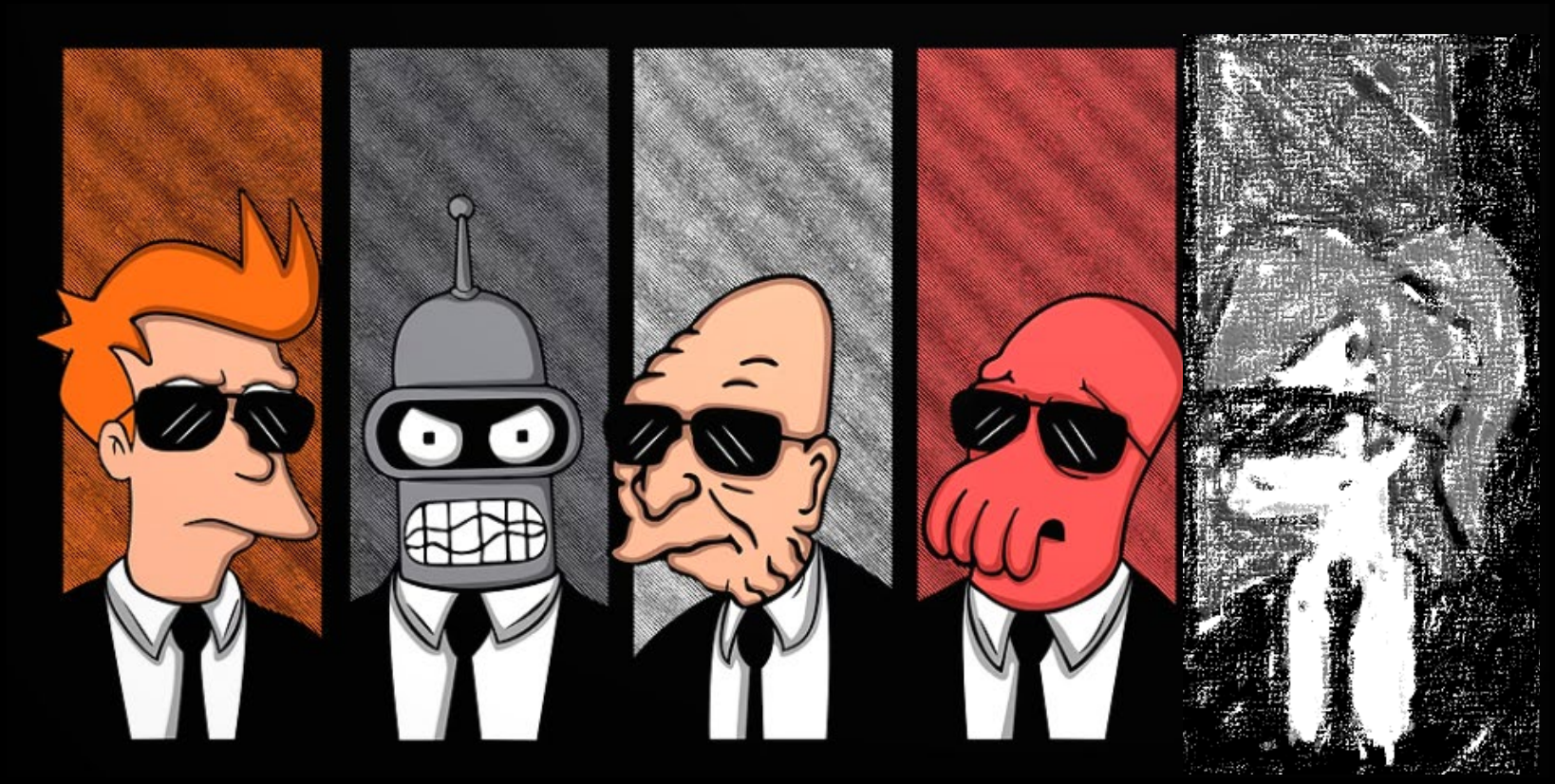
AuthN & AuthZ | Input Val. & Sanit. | HTTPS & Data Encrypt. | Rate Limit & unDoS | Monitoring & Audit

HTTPS и шифрование данных

Обязательное шифрование трафика (SSL/TLS) и данных при хранении (AES-256).

Без HTTPS ваши данные могут перехватить за секунды

СТРАТЕГИИ ЗАЩИТЫ API



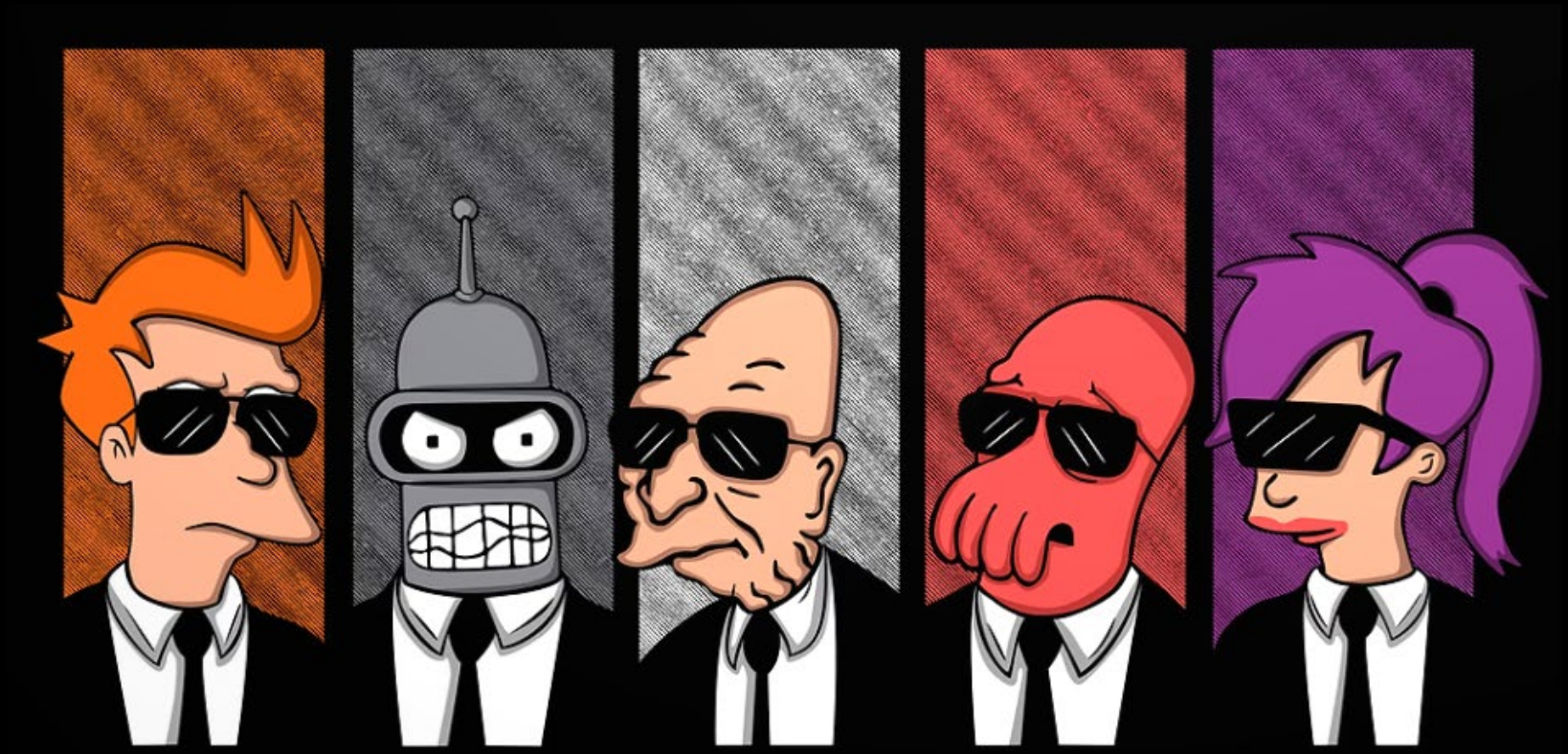
AuthN & AuthZ | Input Val. & Sanit. | HTTPS & Data Encrypt. | Rate Limit & unDoS | Monitoring & Audit

Rate Limiting и защита от DoS

Ограничивайте запросы (например, 1000/час на пользователя) через Redis или Nginx.

Защищает от злоупотреблений и перегрузки сервера

СТРАТЕГИИ ЗАЩИТЫ API



AuthN
& AuthZ

Input Val.
& Sanit.

HTTPS &
Data Encrypt.

Rate Limit
& unDoS

Monitoring
& Audit

Мониторинг и аудит

Отслеживайте запросы, ошибки и аномалии через Prometheus/Grafana или ELK-стек.

Позволяет быстро обнаружить атаку или сбой.

БЛАГОДАРЮ ЗА ВНИМАНИЕ

@PM_VITALIY