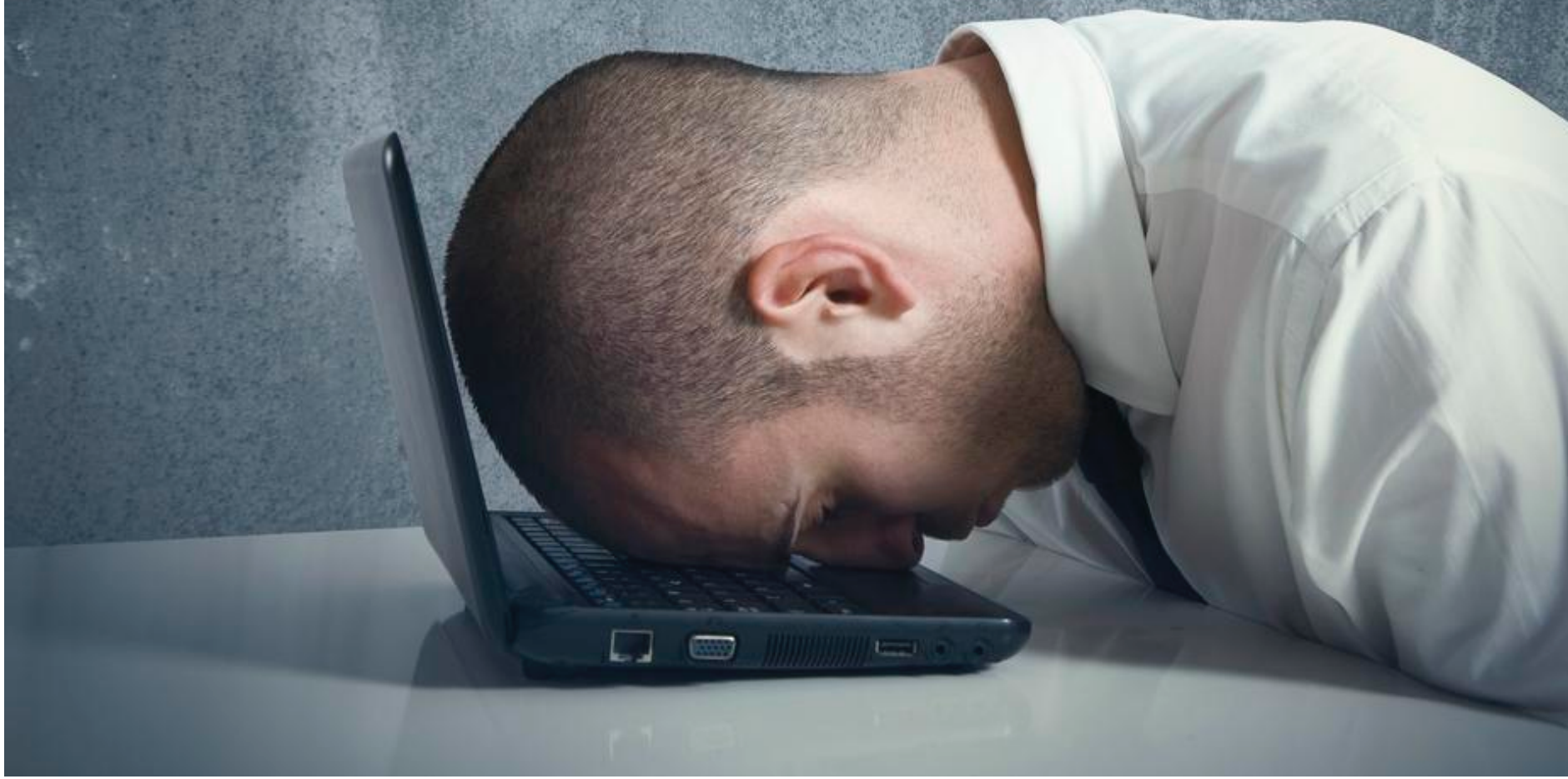
API BEST PRACTICES

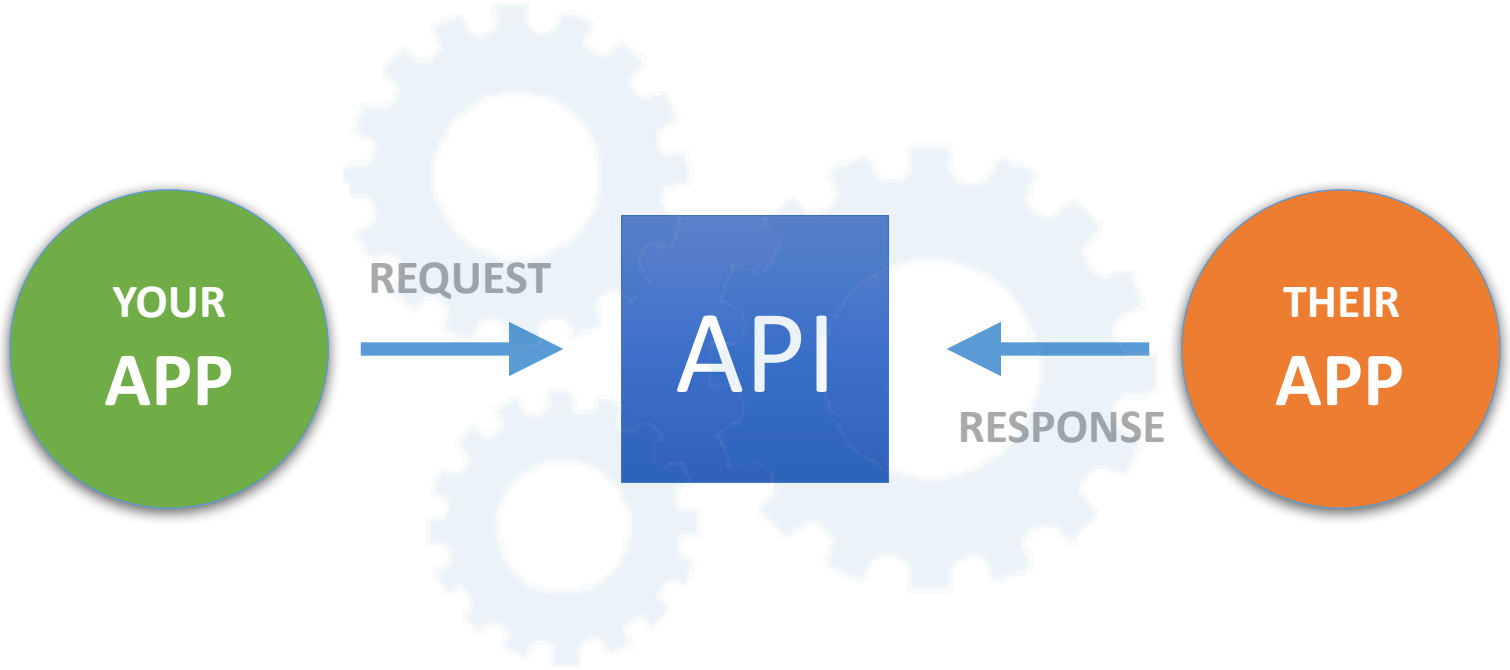
Srikanth Nandiraju
INDX TECHNOLOGY

A Company Without APIs Is Like A Computer Without Internet

Brian Koles



What is an API ?


YOUR
APP
REQUEST
API
RESPONSE
THEIR
APP

An

is a business capability delivered over the Internet to internal or external consumers

- Network accessible function
- Available using standard web protocols
- With well-defined interfaces
- Designed for access by third-parties

What is API lifecycle ?

What is API lifecycle ?

Design

Security

Testing

Partner Portal

Analytics

Operations

API Design

ONE SIZE DOES NOT FIT ALL

API Design

Spec-driven development

- Define the service Interface.
- JSON based (existing or new)
- Decoupled from client & server implementation
- Machine readable (generates documentation & console)
- Language agnostic

standardizing on how REST APIs are described

API Design

- Easy to consume API
  - Noun based URL not Verb based.
  - Use JSON. A gold Standard.
  - Expressing relationships as links. Less to learn, no need to hunt documentation.
  - Query URL's more readable, more intuitive, and easier for API developers to implement. Ex https://dogtracker.com/persons/{personId}/dogs
  - Good error handling design. Devs depend on well designed errors for troubleshooting and resolving issues.
  - Use standard HTTP status codes and complete HTTP response. GET to get data, PUT/POST to change data, etc. Use same general endpoint structure through
  - KISS
- Pick the right API versioning approach
  - The most semantic and clear way to express a version is to put it in your URL, like this: api/v2/Orders


SECURITY

API Security

- OAuth2 and two-way TLS on all critical APIs
- Use domain restriction
- Log all API interactions across channels to get an end-to-end view of user, device and app activities.
- Known threats (OWASP) & unknown threats
- The Open Web Application Security Project (OWASP)
    - XML/JSON injection threats, cross-site scripting attacks, broken authentication, insecure direct object reference, and several others
- Create API proxies using API management tools & enforce a set of consistent security policies at the API proxy layer. Most API-M tools do this out of the box.
- Prevent volumetric attacks. Spike arrest & rate limiting policies - DDoS attacks
- Protect against adaptive threats. API's are programmable so bots can do brute force. AI based algorithms that can analyze billions of API calls can identify and tag bots vs humans. API-M can be used to blocking, throttling or honey-potting.


TESTING

API Testing

- The API lifecycle should be aligned with the SDLC process (Dev, Test, prod)
- Test for backward compatibility
- Plan & Organize test cases to improve productivity, effectiveness and maintenance
- All tests for a given API should be in a single file (named after API).
- Each test case should be as self-contained and isolated from dependencies as possible.
- Test cases should be grouped by the test category (straight-line cases, boundary cases, null inputs, and so forth).
- Try to avoid "test chaining" .
- Use mocking, stubbing & virtualization as needed.

PARTNER PORTAL

API

Partner Portal

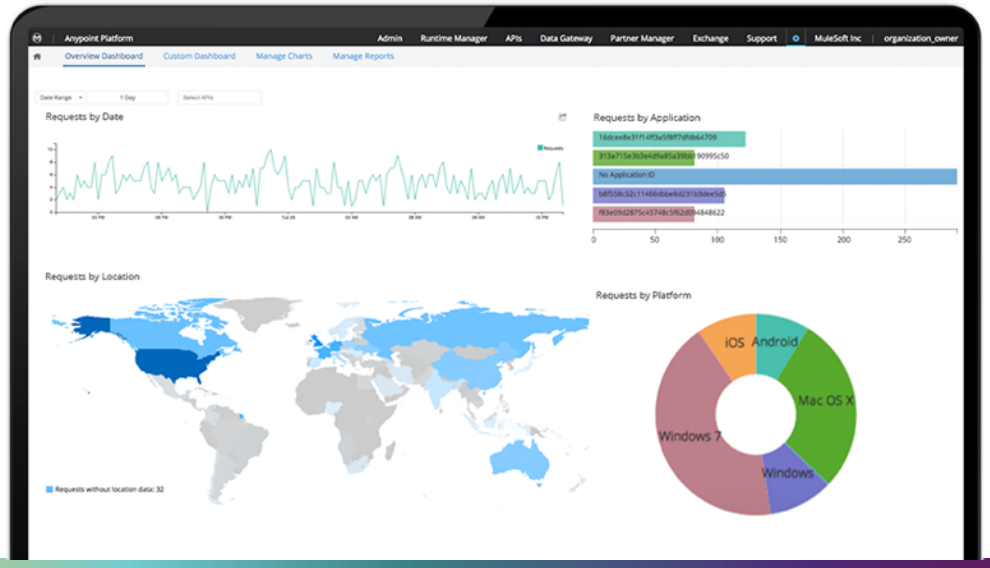
- Create portal for making API discoverable.
- Enable self service capabilities
  - Signup
  - Register app
  - get keys
- Admin approved or Admin Led on boarding
- Easy-to-user API’s with interactive documentation
  - Sample request / response
  - API usage help
  - Guides etc
  - Developer communities.
- Use automatic documentation generation tools like Open API Spec

ANALYTICS

API

Analytics

- Measure, analyze and act on metrics of
  - API traffic trends by products, app developers, and apps
- Trends in signups of new app developers and apps registered for each of their products
- Revenue or business value delivered for each of their published APIs
- Most prolific or highest-value developers
- Developers who are consistently exceeding their quotas




OPERATIONS

API

Operations

- Integrate API management into enterprise operations
- API-M deployment to public , private or Hybrid cloud depending on the enterprise requirement
- API-M can do health check API’s and performance monitoring
- Logging and log analysis.
- Cashing
- Enable security policies for known threats

Thank You. Questions ?