

Mining Security Documentation Practices in OpenAPI Descriptions

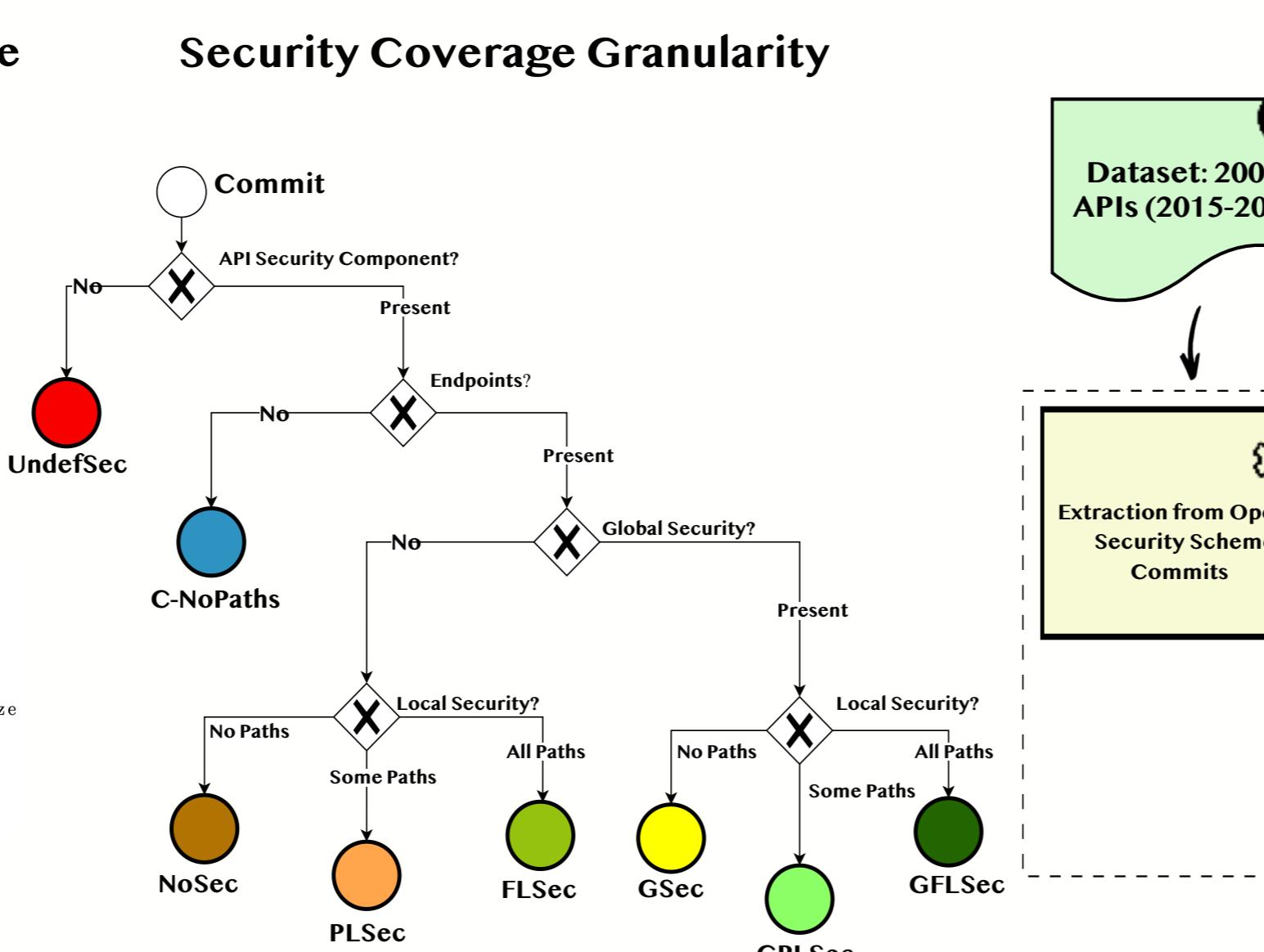
Research Questions:

- R1. To what extent are security aspects documented in Web APIs described using Swagger 2.0 or OpenAPI 3.0?
 - R2. How does the level of detail in security documentation within OpenAPI descriptions vary along API histories?
 - R3. How does security coverage correlate with API size and evolve over time?

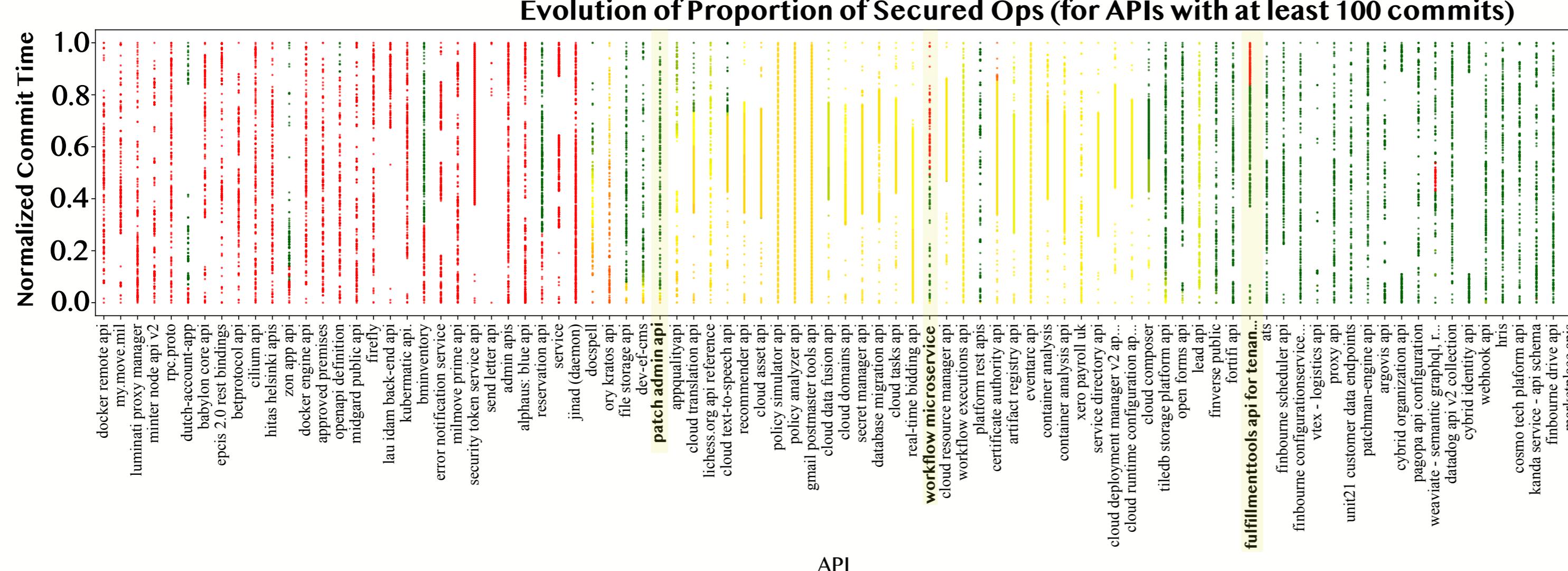
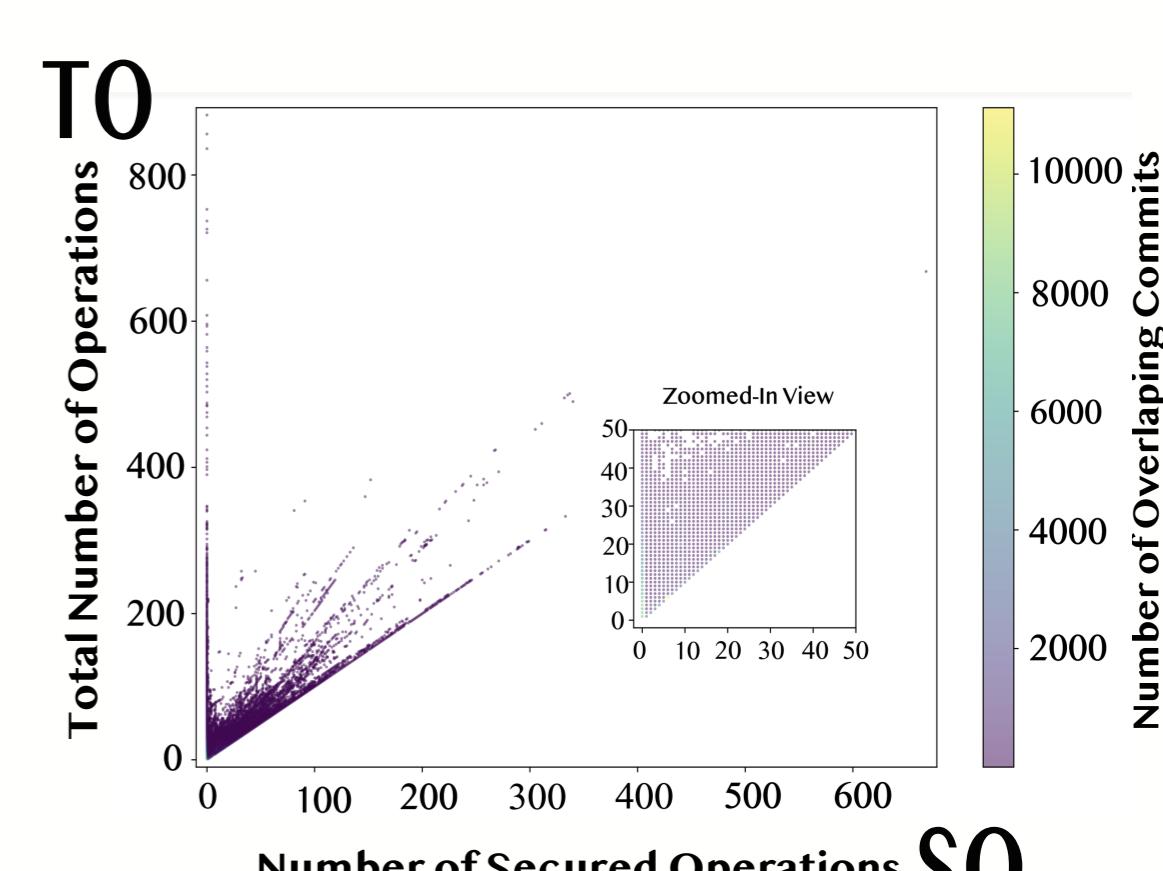
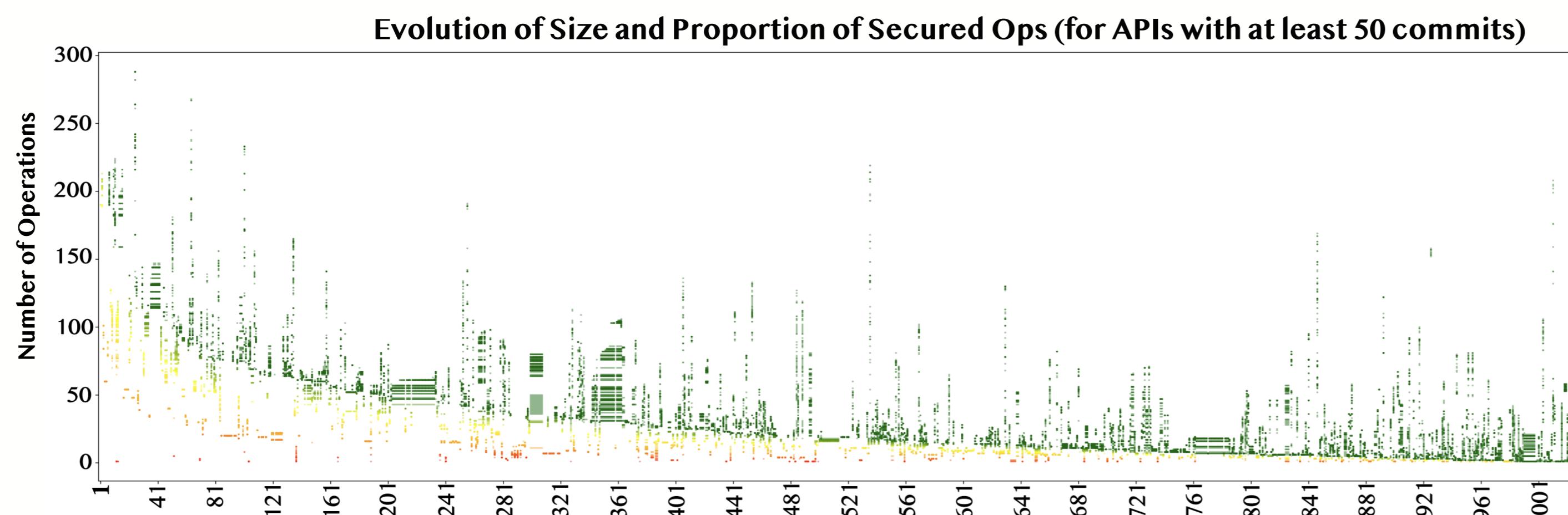
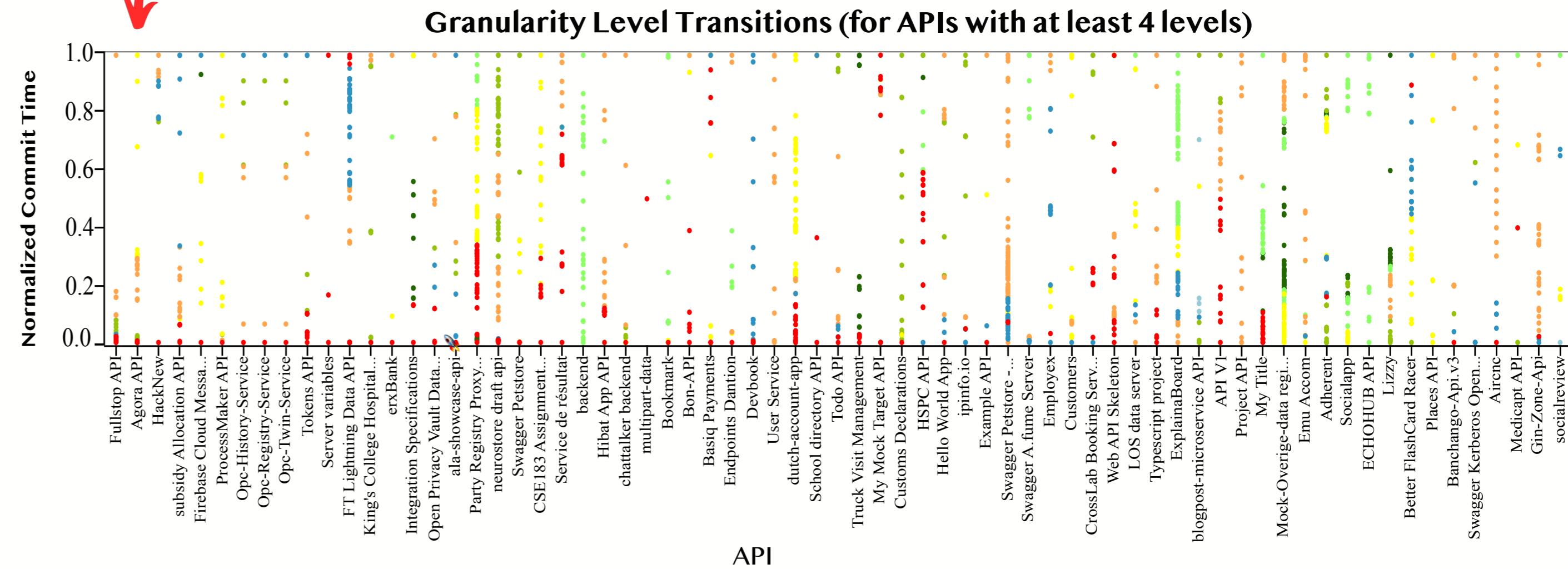
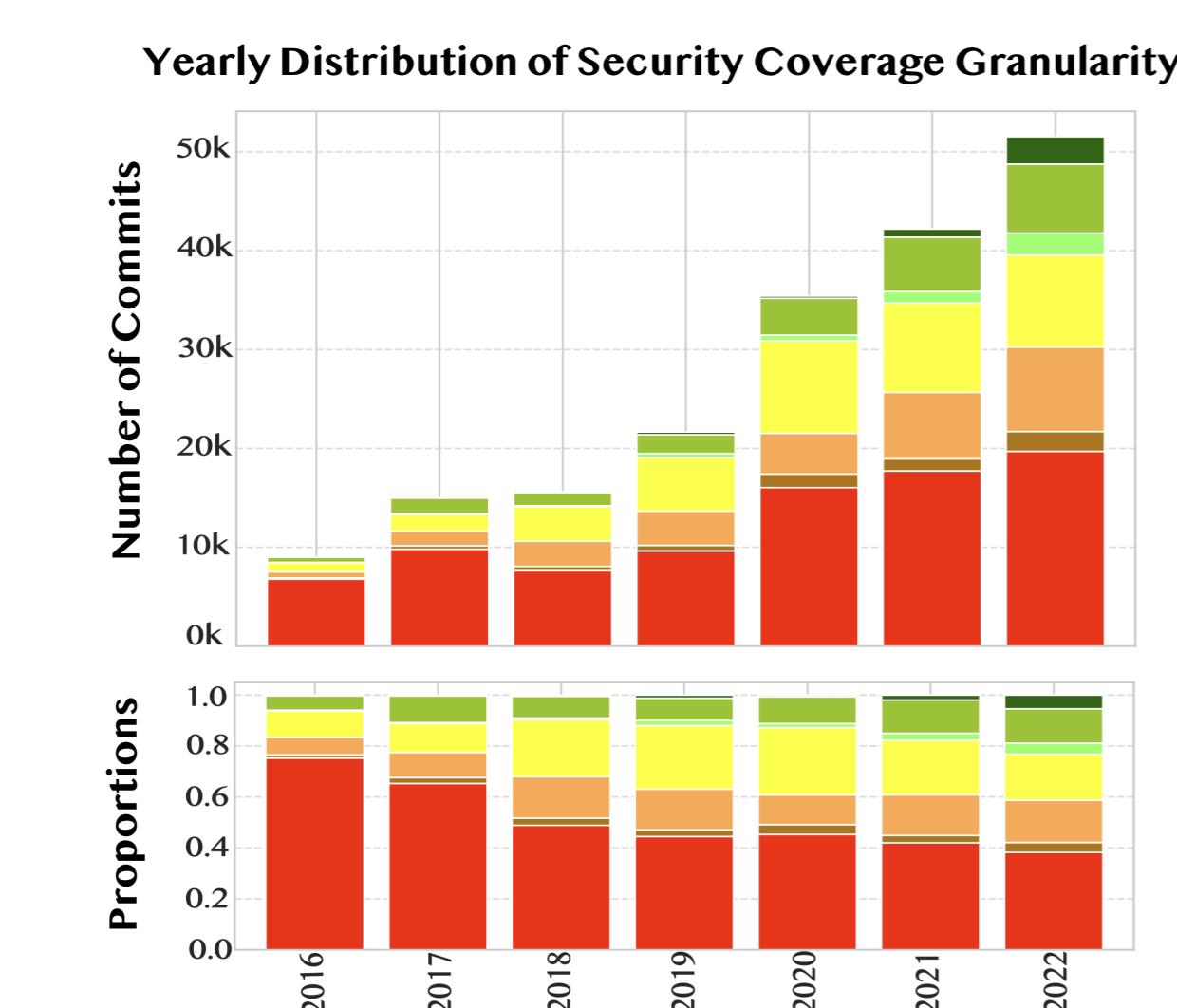
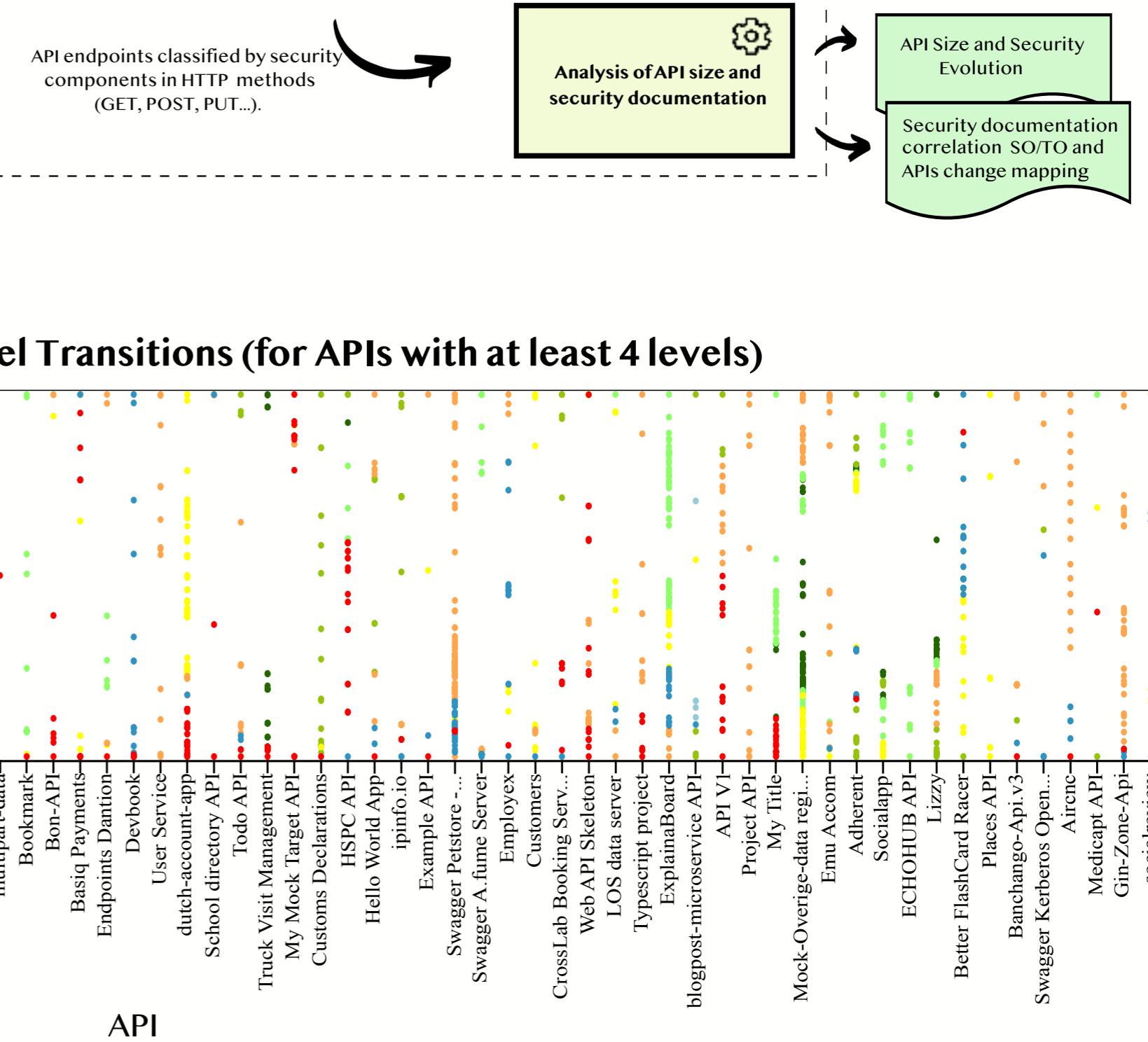
OpenAPI Specification - Input Example

```
openapi: 3.0.3
info:
  contact:
    email: support@socialmedia.com
  title: Social Media API
  version: 1.0.0
security:
  - OAuth2: [read, write]
paths: ...
  /posts:
    get:
      security:
        - OAuth2: [read]
    post:
      security:
        - OAuth2: [write]

components:
  securitySchemes:
    OAuth2: # Custom name for the OAuth2 security scheme
      type: oauth2
      flows:
        authorizationCode:
          authorizationUrl: https://socialmedia.com/oauth/authorize
          tokenUrl: https://socialmedia.com/oauth/token
          refreshUrl: https://socialmedia.com/oauth/refresh
          scopes:
            read: Read access to user's posts
```



OpenAPI Security Analysis Pipeline



$$SOC = \frac{SO(api)}{TO(api)}$$