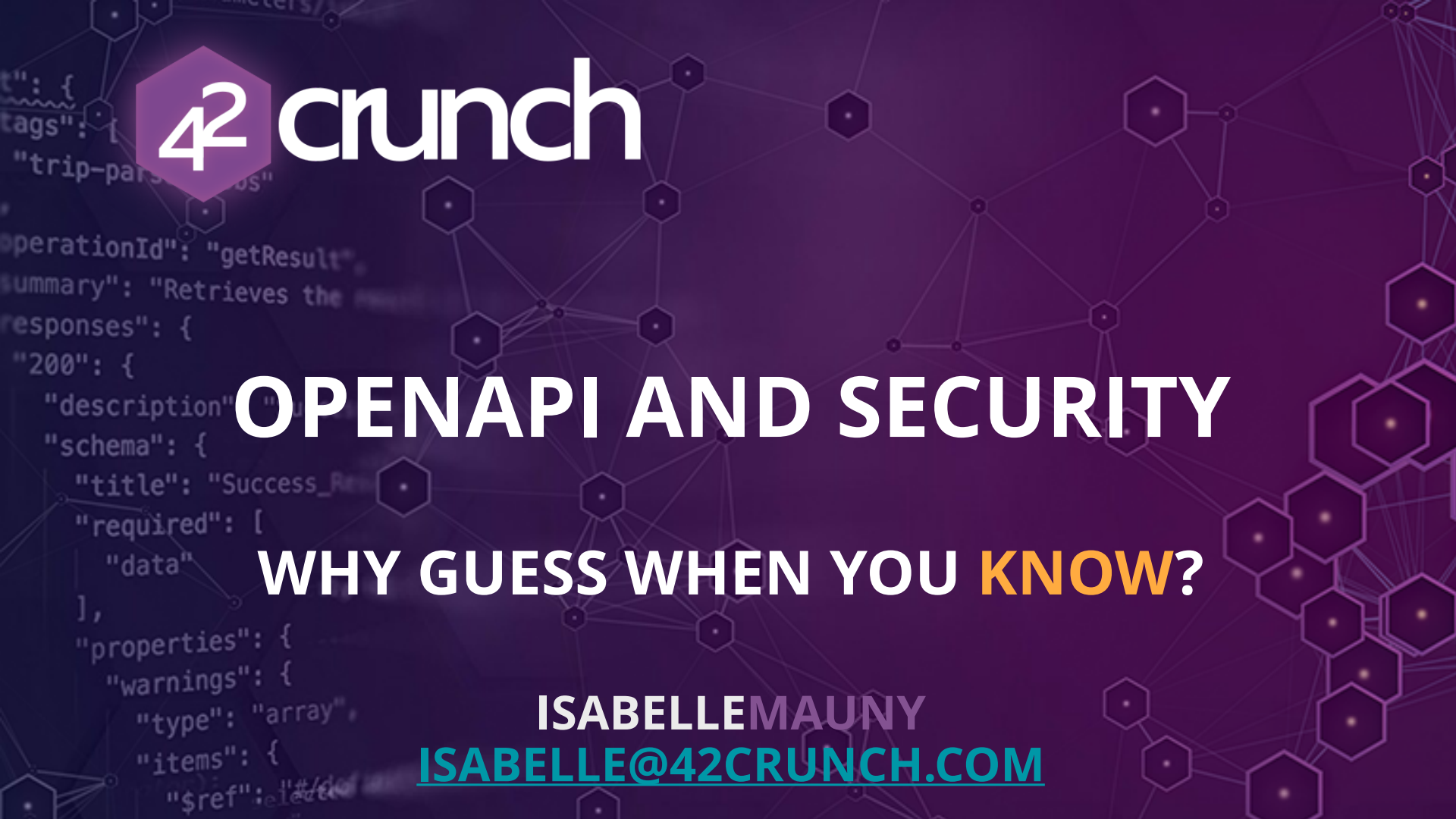
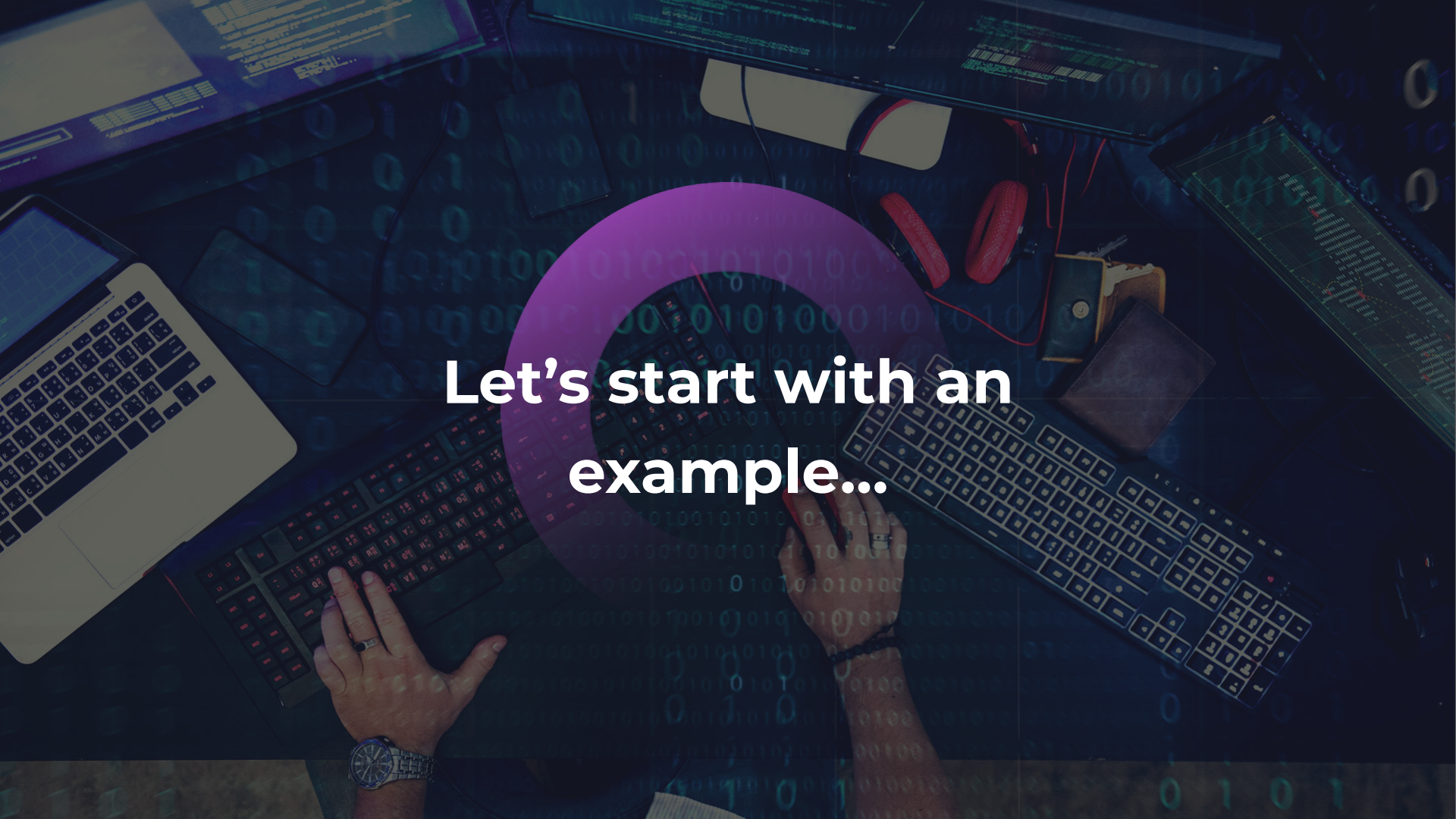


ISABELLEMAUNY
ISABELLE@42CRUNCH.COM


Let’s start with an
example...

STARBUCKS (JUNE 2020)

HTTPS://SAMCURRY.NET/HACKING-STARBUCKS/

- Read the write-up!
- Hacker pokes around to find problems
  - ✓ Test many (invalid) paths
- Finds valid calls from Starbucks website
  - ✓ Try to get to the root of the API to navigate down
- Finds a path that tricks the WAF

```
GET /bff/proxy/stream/v1/me/streamItems/web\..\.\..\ HTTP/1.1
Host: app.starbucks.com
```

- From there, he starts making calls that are present in the API, but must not be accessible directly

Hacking Starbucks and Accessing Nearly 100 Million Customer Records

IN THE END...

Expected:

```
GET /bff/proxy/stream/v1/me/streamItems/:streamItemId HTTP/1.1
Host: app.starbucks.com
```

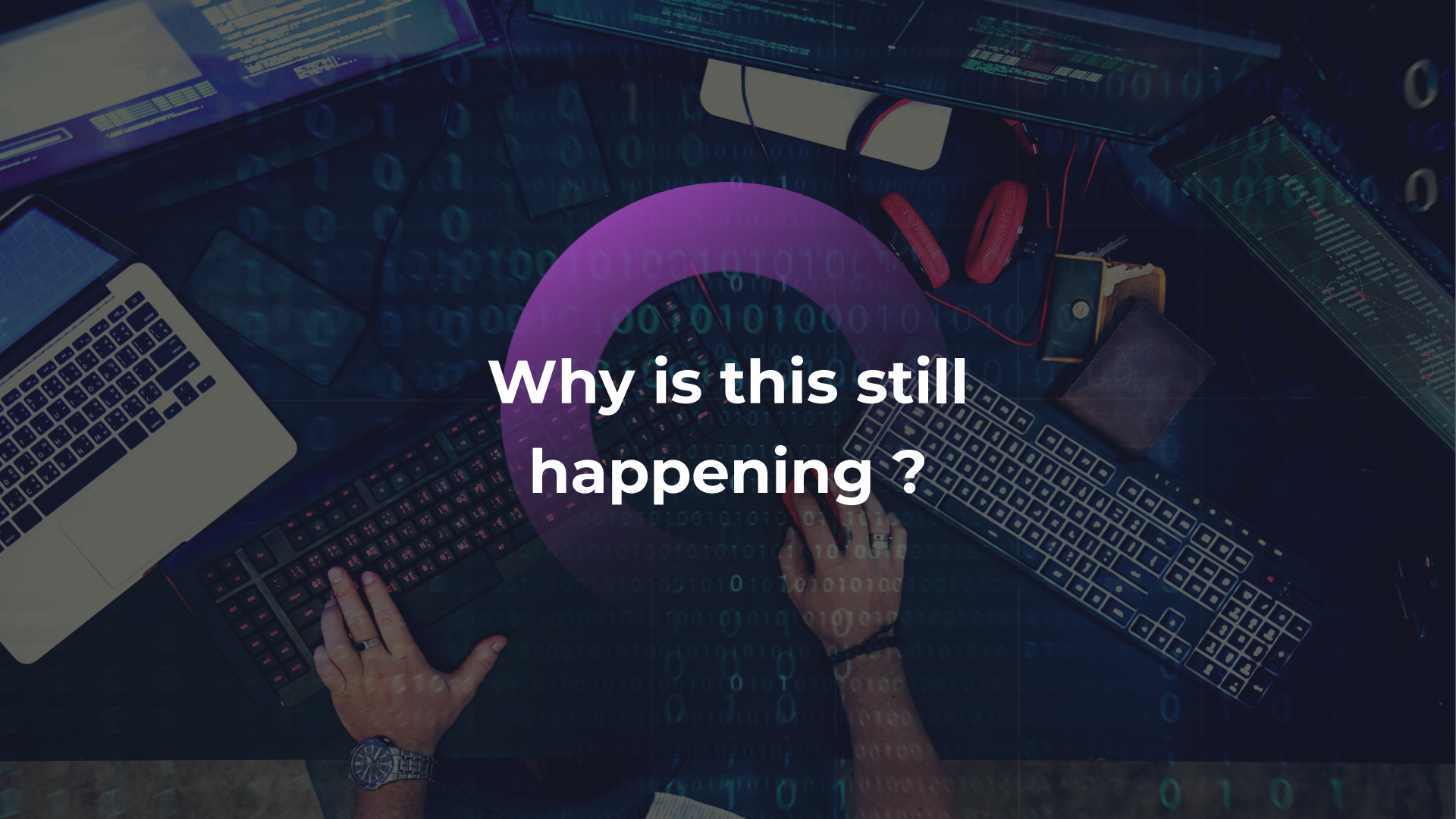
What the hacker was able to call:

```
GET /bff/proxy/stream/v1/users/me/streamItems/web\..\.\..\.\..\.\..\.
\..\.\..\.\search\v1\Accounts\ HTTP/1.1
Host: app.starbucks.com
```

HACKERS USE TRIAL AND ERROR

- Try all verbs
- Try resources names (admin, users, profiles, teachers, accounts, search, ...)
- Try Content-Types
- Inject data (mass assignment)
- Use answers to find info and guess even more

- Check this enlightening video : https://www.youtube.com/watch?v=qqmyAxfGV9c !


Why is this still
happening ?

We are still trying to guess...

- Web Application Security is painful because the security is not handled from beginning
- Developers cannot define how the web application is built and designed
- After 20 years of R&D, detection and protection tools have to use AI to understand how the Web Application works...


Is there another way ?

POSITIVE SECURITY MODEL

Access Denied by default

Allow Access only to approved traffic

Trust centric

WHY A POSITIVE MODEL ?

- Much stricter access control
- Limited false positives
- No need to update when new threats are found
- You're protected even if new rules have not been created to detect the new threats.

KEEPING UP IS HARD...

- An allowList is only powerful if complete!
- It requires lots of efforts to define and maintain up to date with constant applications changes
  - ✓ High human cost, usually several people full time
- Traditionally been very hard to implement
  - ✓ Which is why the default WAF model is to use a denyList

OPENAPI INITIATIVE

3scale BY RED HAT
42crunch
ably
Acumatica The Cloud ERP
APIFORTRESS
APImetrics API INTELLIGENCE
Assertible
ATLASSIAN
Band Protocol
Bloomberg
ebay
Google
HM Government
IBM
IFS
Intento
Interzoid
isa
Kong
Liferay
LinksRez
Microsoft
MuleSoft
NHS
opentravel enabling the future
ORACLE + apiary
POSTMAN
RepreZen
SAP
SMARTBEAR
software AG
Stoplight
talend
TeejLab
TORO CLOUD
Tyk

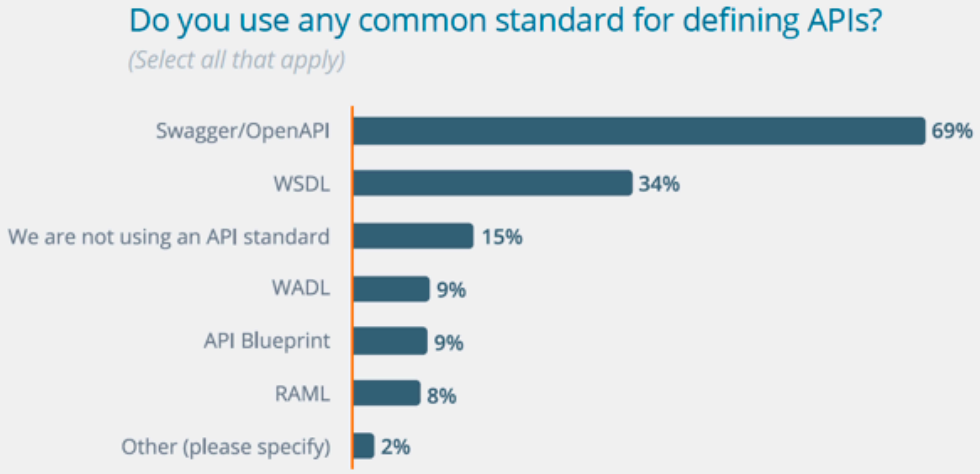
WHAT IS THE OPENAPI SPECIFICATION (OAS) ?

- The OAS lets developers describe a REST API contract in a programming language-agnostic way
- Traditionally used to document APIs for internal and external consumption
- Core component of **API First Design** (API is defined before the API implementation is done)

SPECIFICATION ADOPTION: FROM 25 TO 70 % IN 3 YEARS

The OpenAPI Specification is the de facto standard for API design

69% of respondents are using the OpenAPI Specification (OAS) in their API development. OAS was the clear favorite standard for RESTful APIs, with other REST-based standards — API Blueprint and RAML — only accounting for 16% of respondents. OAS was only used by 25% of respondents in the 2016 State of API Survey. The explosive growth in OAS adoption can likely be credited to the release of OAS 3.0 in 2017, which was the first official release of the OpenAPI Specification since being donated to the OpenAPI Initiative in 2015, as well as the expansion in tooling support for OAS. It's clear that the industry is rallying around open standards over propriety standards.



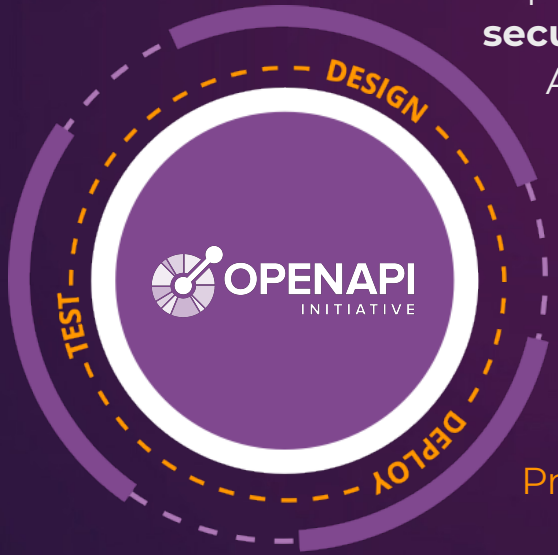
What is the main way changes and feedback are

ADOPTION

- Mandated by many large companies as the standard to describe all APIs (produced internally or via outsourcing).
- Critical business APIs, such as eBay, Stripe, GitHub, Paypal, Box all use OpenAPI to describe their API contracts.
- apis.guru now references 600+ public APIs described with OpenAPI. APIs from Amazon, Microsoft, Atlassian, Cisco, Citrix, Docusign, Google are referenced on this site.
- Largely supported by OpenSource community tools (https://swagger.io/tools/open-source/)

HOW 42CRUNCH LEVERAGES OAS

Audit Service performs **200+ security checks** on API Contract



Scan service ensures API implementation **conforms to API contract**

Protection service is **automatically configured** from API contract


Do we need AI for other
type of issues ?

BEHAVIOURAL ANALYSIS

- We use AI to analyse the navigation patterns of the user within the API
  - ✓ /Login , then /listAccount then getAccountDetails
  - ✓ if somebody starts to only call getAccountDetails, enumerating accountIDs, we flag it.
  - ✓ Hacker starts “poking around”
- Benefits
  - ✓ Detect bad behaviours automatically (in a massive number of requests)

DATA DISCOVERY

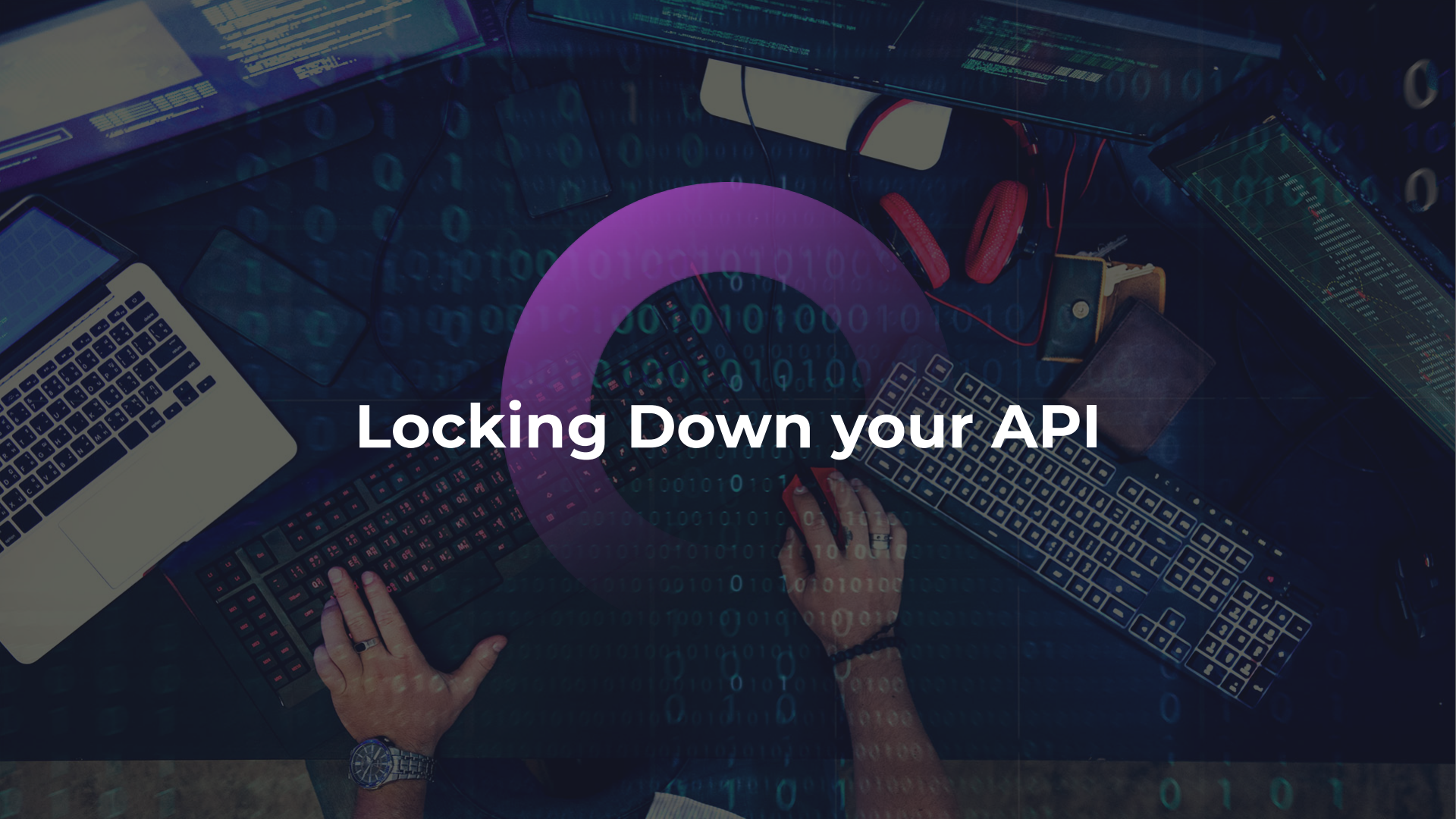
- Analyze traffic to enhance / discover APIs
- Discover data formats and flag inconsistencies with existing contract
- Benefits
  - ✓ Flag inconsistencies across many calls for data where having a pattern might be difficult or inefficient

FEW THINGS TO REMEMBER ABOUT AI

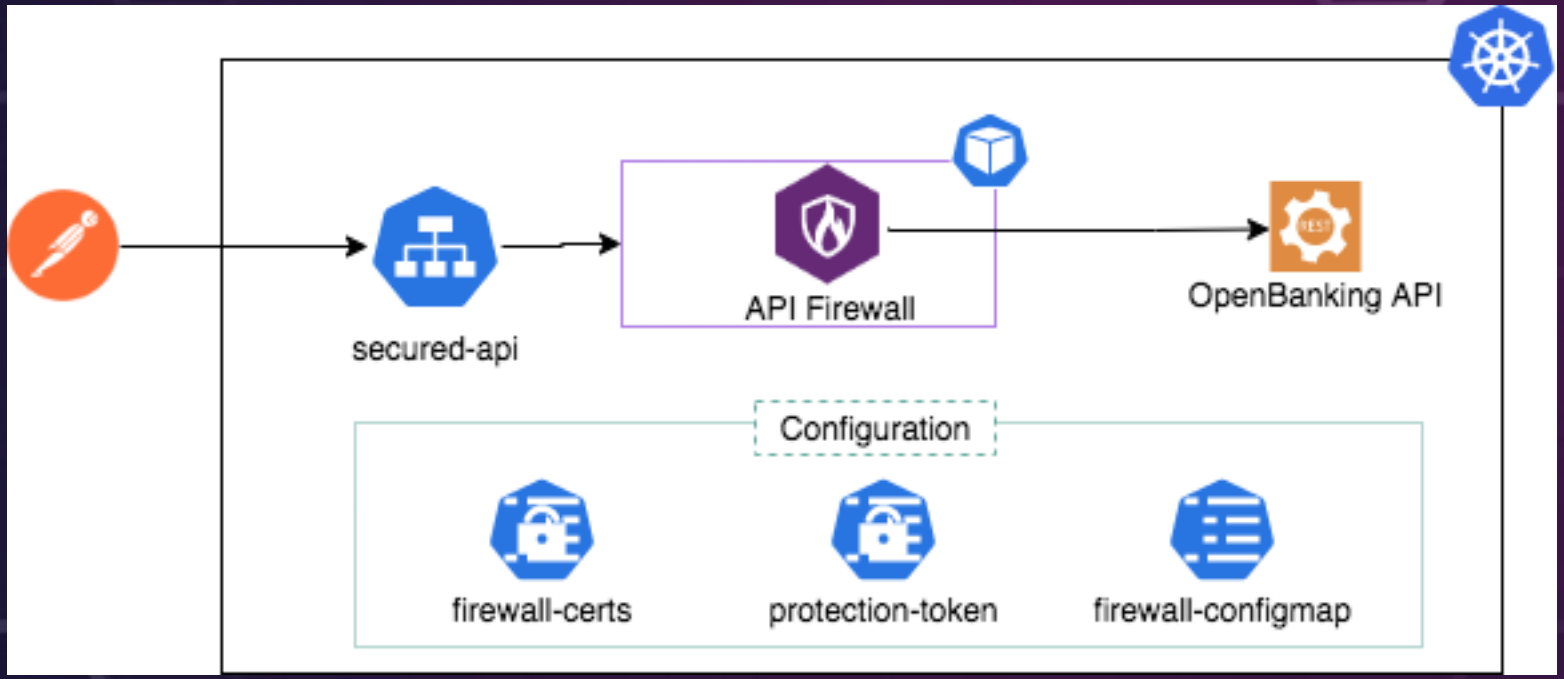
- It's all about statistics...will never be 100% sure
- It needs data to calculate that probability
  - ✓ Won't stop anything on first bad request
  - ✓ Will need quite a few of those to detect problems and raise alerts
- Every API is unique, so it needs to be trained for each of your APIs (and with production data)
- Most likely won't work well if you have low traffic
- Can give recommendations and raise alerts, usually won't stop traffic (as its statistics based!)

BUT MORE IMPORTANTLY…

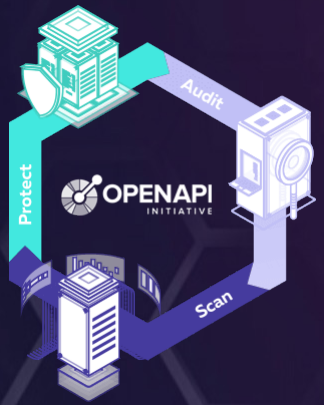
- If something is blocked , If something is not blocked
  - ✓ Can you explain why ?
- If a hacker is detected, you ban their IP
  - ✓ And they will create another…and another…


Locking Down your API

DEMO SETUP



WHY POSITIVE SECURITY?



Cover the basics first...

Validate

- Use a positive security approach to discard any unwanted requests/ responses

Use standards

- OpenAPI can help you standardize across all your teams

Automate Security

- Audit security and deploy protections automatically as early as dev time.


42 crunch
CONTACT US:
INFO@42CRUNCH.COM
Start testing your API contracts today on apisecurity.io!

RESOURCES

- 42Crunch Website
- Free OAS Security Audit
- OpenAPI VS Code Extension
- OpenAPI Spec Encyclopedia
- OWASP API Security Top 10
- APIsecurity.io