42crunch

apidays LIVE LONDON

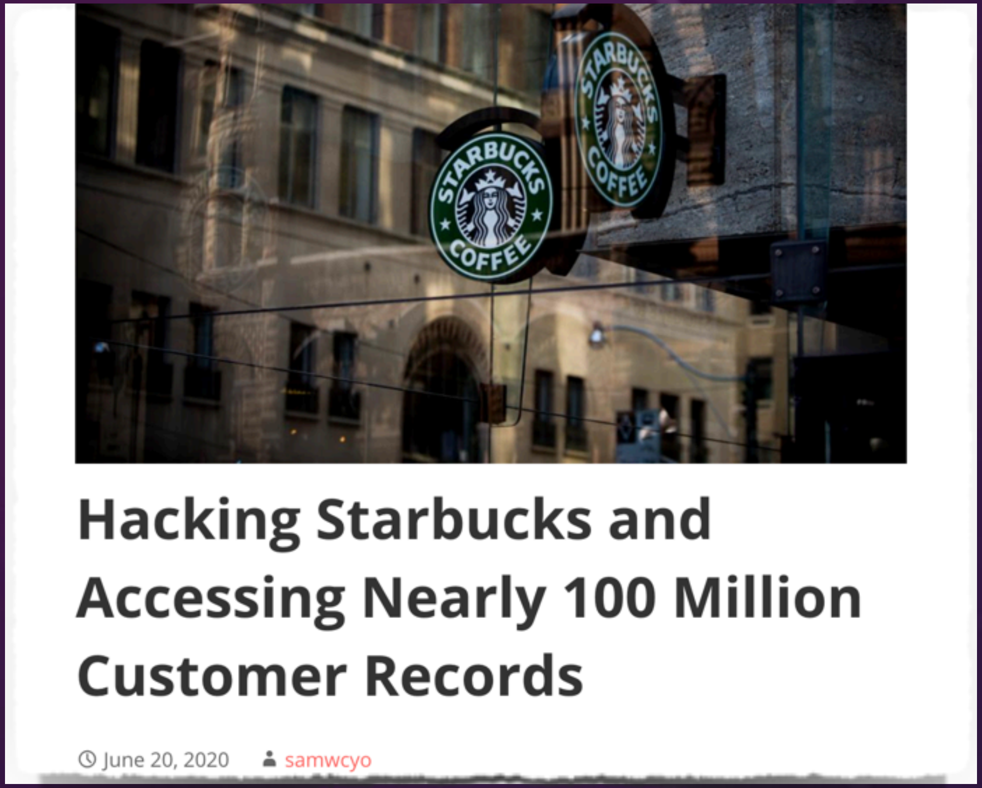
EU Commission Workshop

API Essentials

ISABELLE MAUNY
ISABELLE@42CRUNCH.COM

API Breaches are on the rise!

- 300+ breaches reported on apisecurity.io since Oct. 2018
- And those are just the public ones!
- Most recurrent causes (combination of):
  - Lack of Input validation
  - Lack of Rate Limiting
  - Data/Exception leakage
  - BOLA/IDOR (Authorization)



Hacking Starbucks and Accessing Nearly 100 Million Customer Records

June 20, 2020 samwcyo

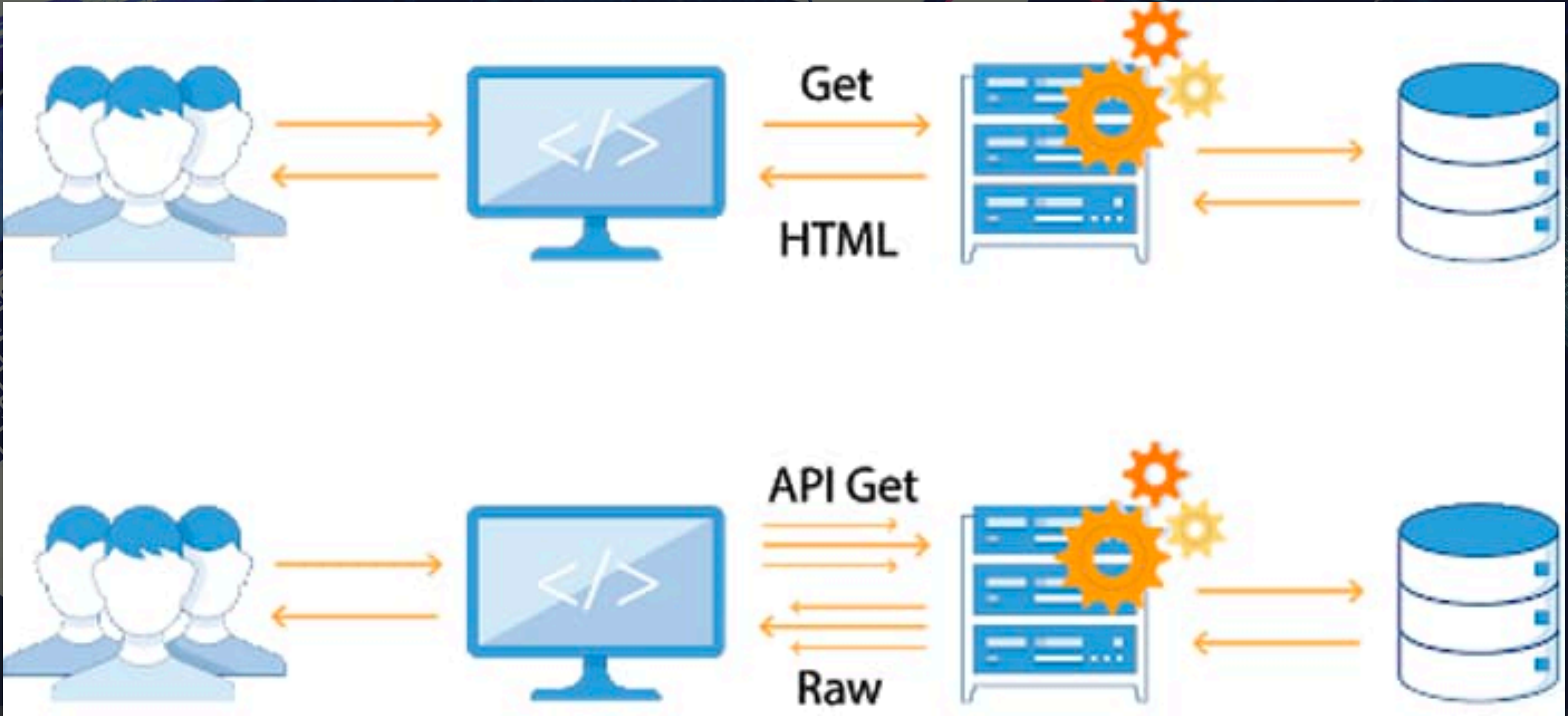
APIs have different vulnerabilities

OWASP API Security Top 10

- API1 : Broken Object Level Access Control
- API2 : Broken Authentication
- API3 : Excessive Data Exposure
- API4 : Lack of Resources & Rate Limiting
- API5 : Missing Function Level Access Control
- API6 : Mass Assignment
- API7 : Security Misconfiguration
- API8 : Injection
- API9 : Improper Assets Management
- API10 : Insufficient Logging & Monitoring

WHY IS THIS HAPPENING?

Applications Architecture has changed!



Source: https://apisecurity.io/encyclopedia/content/owasp/owasp-api-security-top-10.htm

FROM PROTECTING THE PERIMETER…

...TO PROTECTING THE DATA

MANY APIS, DEPLOYED OFTEN

APPLICATION DEVELOPMENT

APPLICATION SECURITY

“The perimeter has disappeared. **It’s no longer about protecting boundaries, it’s about protecting data.**”

To make it worse!

- **API Security is considered too late**
  - ✓Security teams can’t do their job properly
- **API Security is hard**
  - ✓Complex standards, limited skills
- **Each API must be protected individually**
  - ✓ 100’s of specific policies to write

What needs to happen…

Development is **agile** - **Security** must be as well!

Security must **start early** and become fully part of the API lifecycle!

Developers must become become **key actors** of security

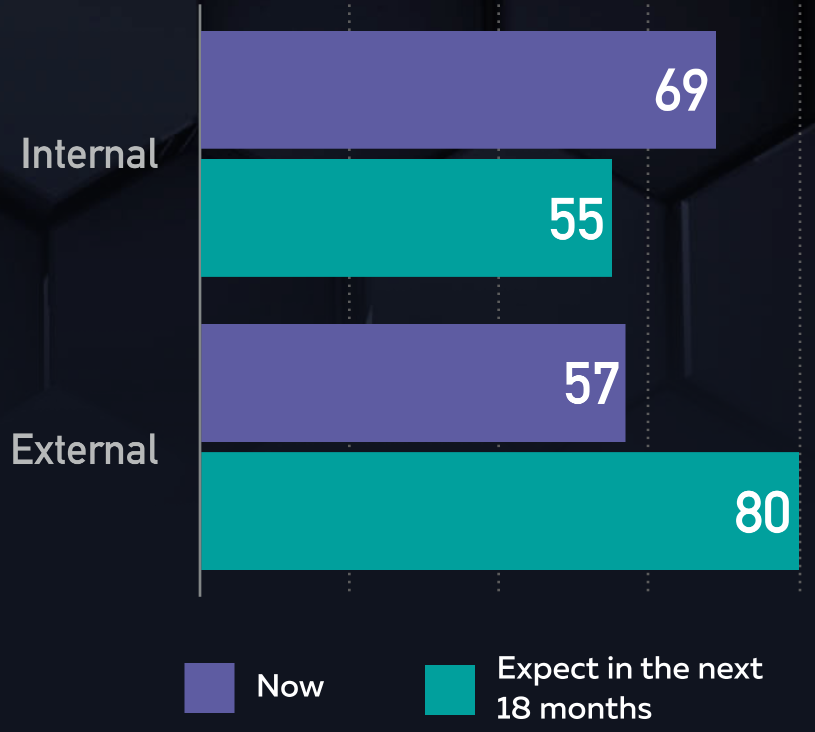
1

ALL APIS SHOULD BE TREATED AS PUBLIC

WHAT ARE APIS FOR ?

EXPOSING ENTERPRISE DATA AND PROCESSES.

Have you experienced the theft or corruption of internal corporate or user/consumer information by Internal or External threat actors?



Source: @ " Accenture
and HIS Research - Sample: 208 Enterprise Security Professionals

KEEP
CALM
AND
TRUST
NONE

> “I think that a lot of people think that because there is **no GUI** on an API that **no one can find it** and it is invisible. **But we can find them in about five seconds** with a proxy…
>
> …**Almost every threat that applies to a web app, can happen to an API**, but a lot of people for some reason are not protecting them as much as their web applications.”

Tanya Janca

Application Security Evangelist - AppSec Podcast

WHAT SHOULD YOU DO ?

- Proceed to a full inventory of APIs within the enterprise
- Implement APIs governance
- Evaluate your API Security coverage

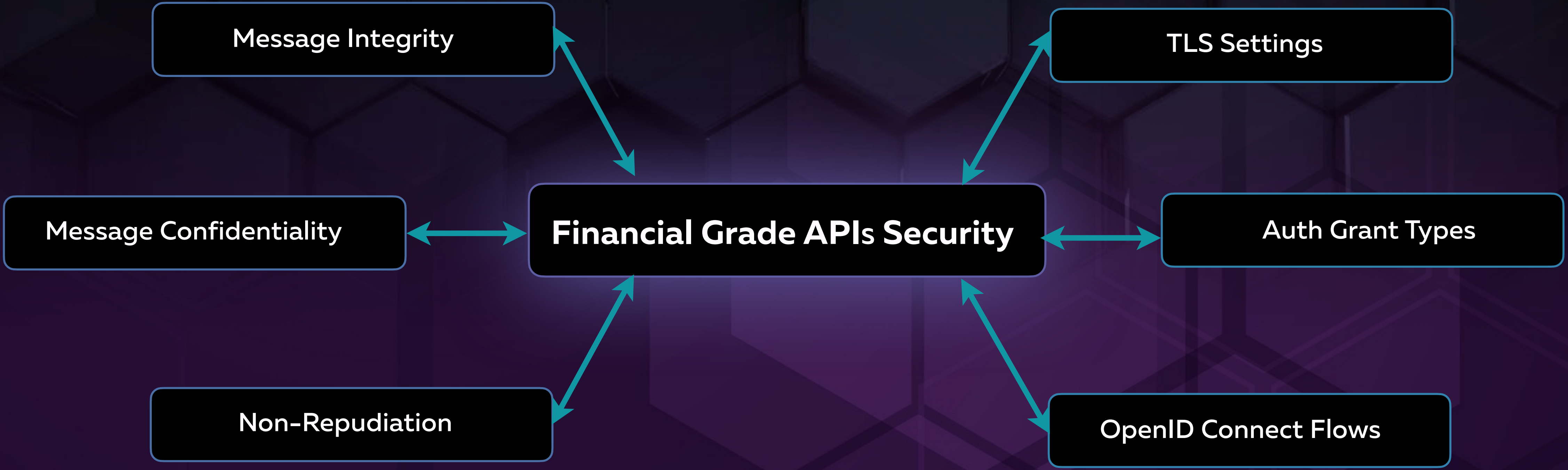
2

SECURITY NEEDS TO BE RISKED-BASED

> “Security is a risk control measure…**In the security sphere, one size does not fit all.** We have to take ‘appropriate measures’.

Nat Sakimura

Fixing OAuth, Nat Sakimura, July 20, 2016, https://nat.sakimura.org/2016/07/20/fixing-oauth/



Financial APIs Working Group: http://openid.net/wg/fapi/

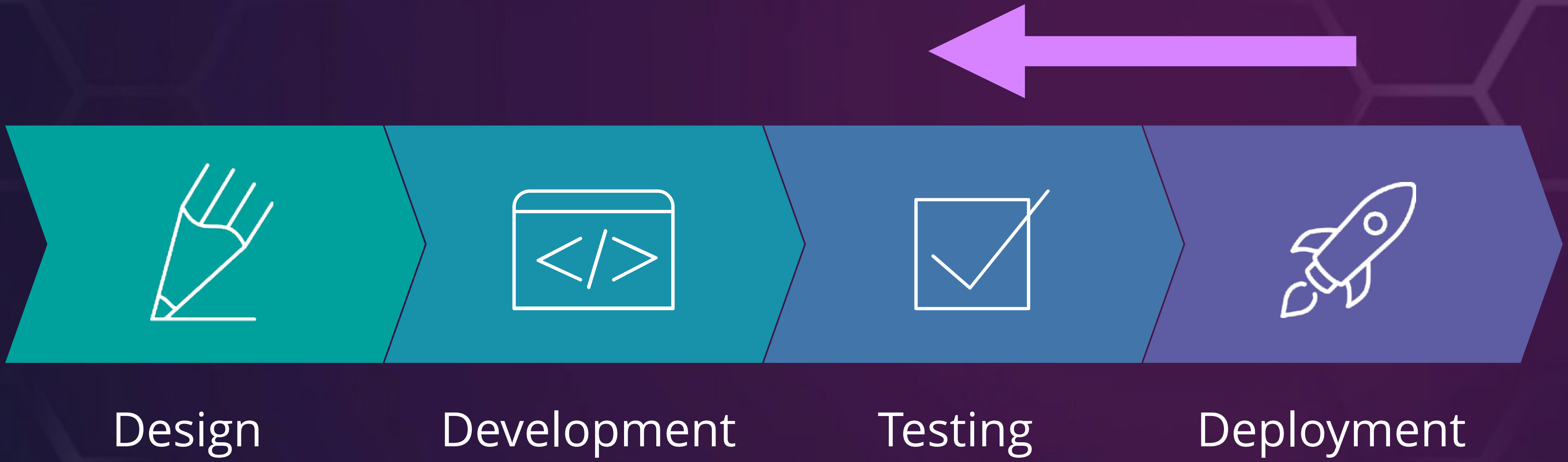
WHAT SHOULD YOU DO ?

- Establish a threat model for all APIs
  - What is the data sensitivity (a.k.a Would I make the news if that data was leaked?)
  - Who is going to access, now and later ?
- Establish corporate security policies based on that threat model, managed by the security teams.

3

SECURITY MUST BE AUTOMATED

INJECTING SECURITY AS EARLY AS POSSIBLE IN THE API LIFECYCLE



SHIFTING SECURITY LEFT

Dev Sec Ops Benefits

- Everyone is responsible for security, everyone has a role to play
  - No more “throwing over the fence” approach
- Vulnerabilities found early take up to **30x less effort** to solve
- Secure by design principles
  - Automated reviews
  - Automated security testing
- Security becomes transparent, thanks to security as code
- Developers iteratively learn about best practices
- Security is continuously improved

IMPLEMENT VULNERABILITY SCANS

- Infrastructure Scans
- TLS + Security Setup
  - ✓ APIs Server, CDN, HTTP Server
  - ✓ Security headers
- Code analysis (Static, Dynamic, Interactive)
- Third-party libs / frameworks
- Apps / APIs (e.g. OWASP ZAP)
- Authentication
- Authorization
- DevOps Scripts!

Choose platforms/tools where functionality is exposed as APIs/CLI.

WHAT ELSE SHOULD YOU DO ?

- Apply security policies as early as possible in the API lifecycle
- Choose a platform where security policies can be applied automatically, with minimum involvement of developers
- Test APIs with “security ON” from Day 1!

FINAL THOUGHTS

- We have best practices and recommendations which work for finance and can be adapted to all industries, including government.
- We need to invest in educating and leveraging the “Development Army”
- We need to act like hackers and start testing APIs for all edge cases
- We need to automate and engrain security into our API development journey.

Thank you!

Contact us | info@42crunch.com | 42crunch.com

Free security tools from 42Crunch

https://42crunch.com/resources-free-tools/