GITHUB CODE SCANNING: What – Why – How

Davide Benvegnu
DevOps Lead & YouTuber

Davide Benvegnu

DevOps & Infra Lead @ PlayStudios

Former DevOps Architect @ Microsoft + GitHub

Former MMA Fighter

@DavideBenvegnu

github.com/n3wt0n

linkedin.com/in/davidebenvegnu

coderdave.io

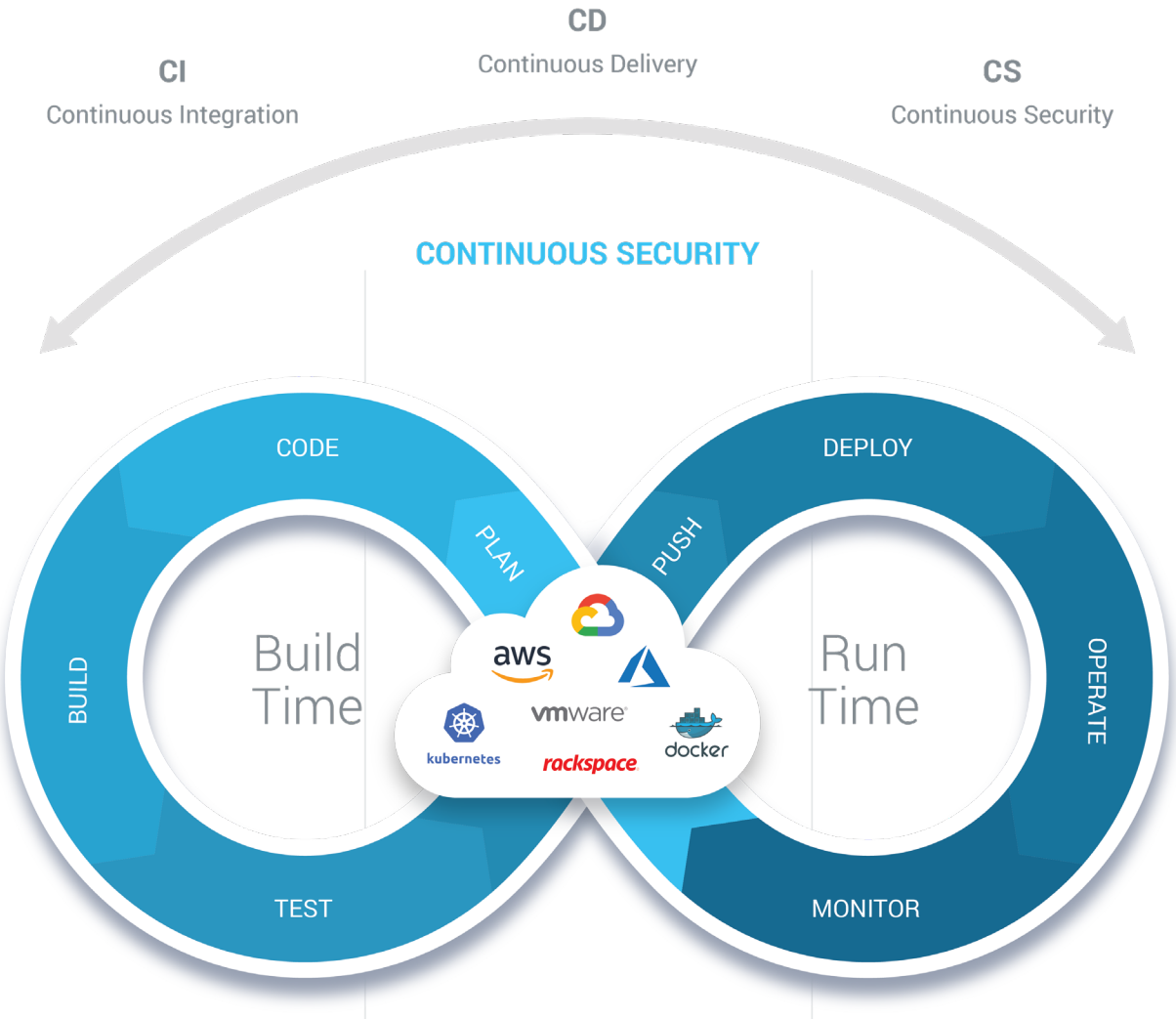
PLAYSTUDIOS

CoderDave

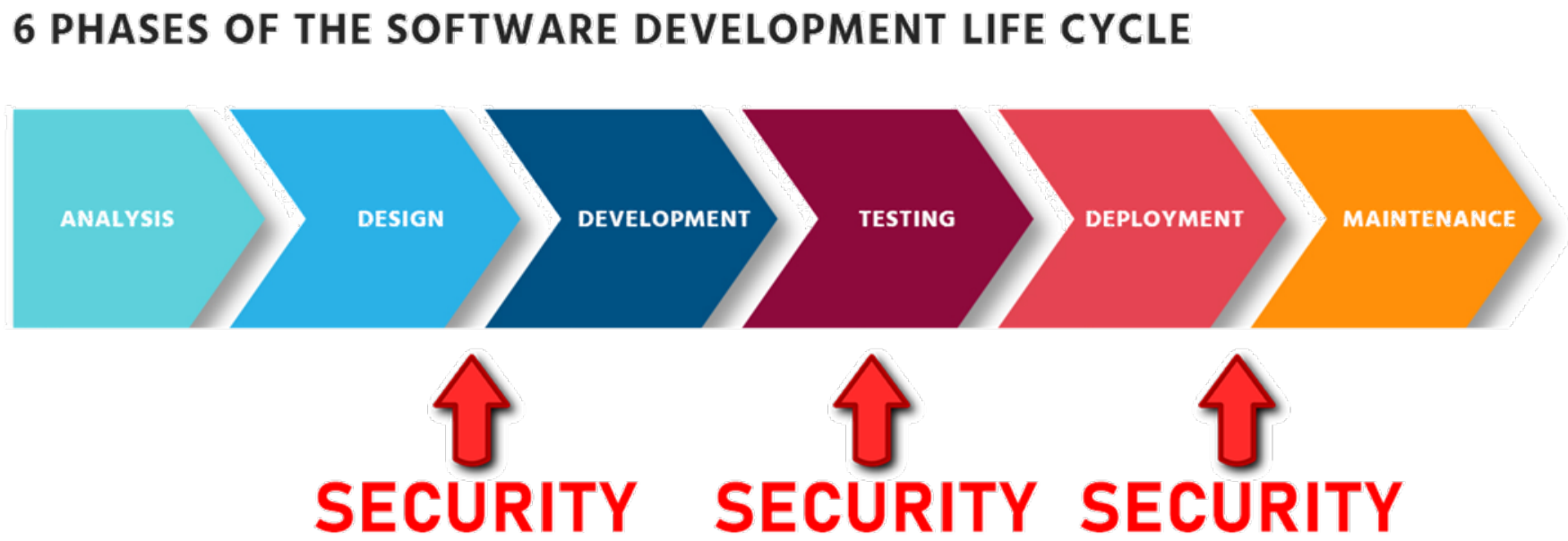
Allegedly Famous YouTuber

Security is important

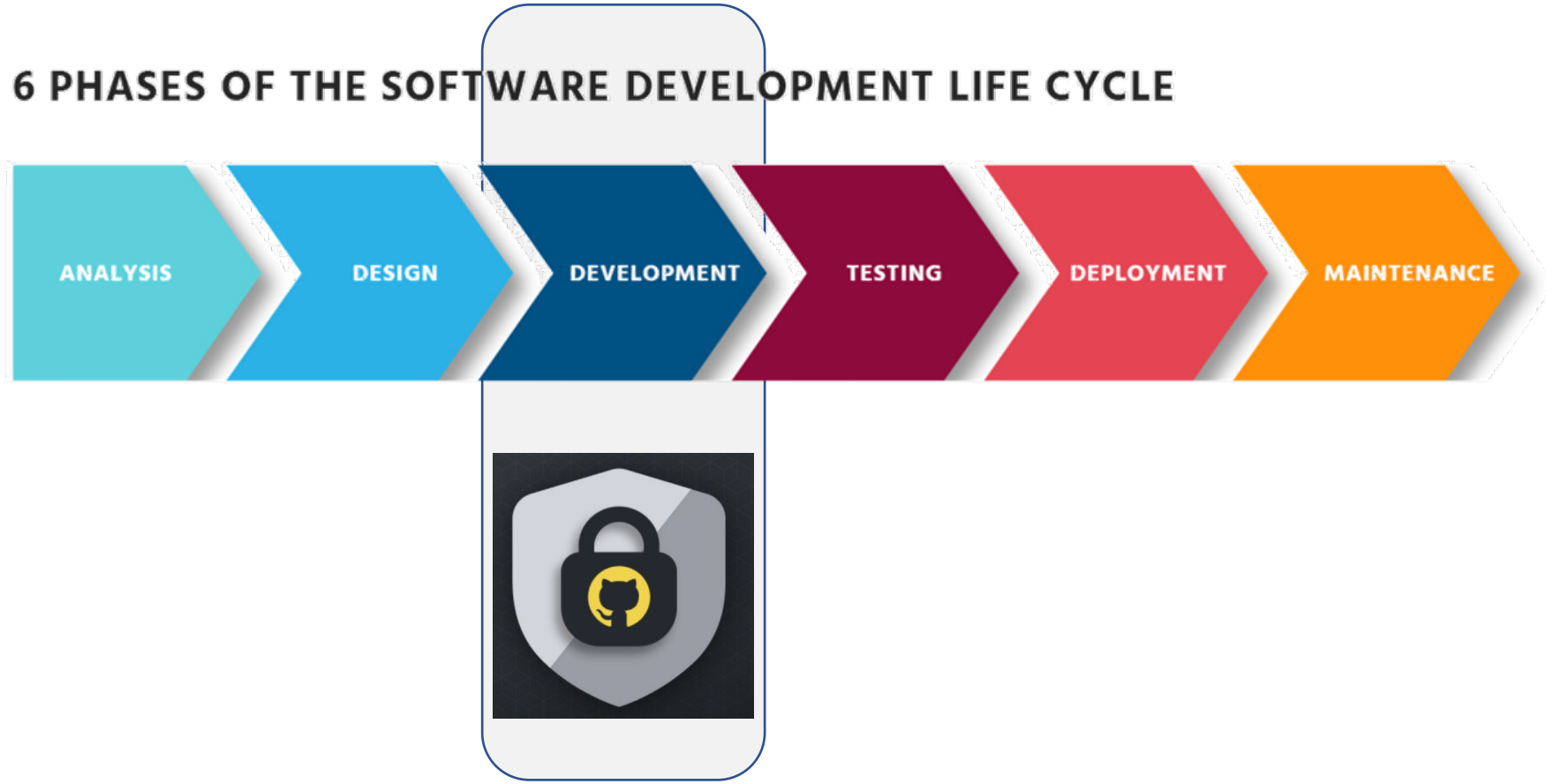
Continuous Security



Shift Left


6 PHASES OF THE SOFTWARE DEVELOPMENT LIFE CYCLE
ANALYSIS
DESIGN
DEVELOPMENT
TESTING
DEPLOYMENT
MAINTENANCE
SECURITY
SECURITY
SECURITY

Shift Left


6 PHASES OF THE SOFTWARE DEVELOPMENT LIFE CYCLE
ANALYSIS
DESIGN
DEVELOPMENT
TESTING
DEPLOYMENT
MAINTENANCE

GitHub Code Scanning

What is Code Scanning

Analyze the code in a GitHub repository to find **security vulnerabilities** and **coding issues**.

Based on **CodeQL**, inherited from Semmle and LGTM

Integrated into GitHub, **interoperable** with third-party code scanning tools that output Static Analysis Results Interchange Format (**SARIF**) data

The 3 flavors of Code Scanning

Native	CodeQL	3rd-party tools
Pre-built GitHub Actions and Actions workflows	Run the **CodeQL CLI** in GitHub Actions or any **3rd party CI** systems	Using GitHub Actions, or
Up and running in **minutes**	**Upload** results to GitHub	**Generated externally** and uploaded to GitHub
Works only in GitHub	Works only with **GitHub-hosted code**	Works only with **GitHub-hosted code**

3rd-party integrations

Code Scanning

Supported Languages
Code Scanning / CodeQL supports both compiled and interpreted languages

- C/C++
- C#
- Go
- Java
- JavaScript/TypeScript
- Python
- Ruby

Quality of Results
- Fairly low false positive ration
- Can catch issues other tools may not

Customizable
- Based on CodeQL queries, regularly updated,
- Open source: https://github.com/github/codeql

- Write your own queries
- Publish a CodeQL query pack (*beta*) to GHCR (self-contained)
- Create a QL pack in a repository

Configurable
- Default config is usually "*good enough*"
- Custom config file

- Disabled default queries
- Specifying CodeQL query packs
- Specifying additional queries

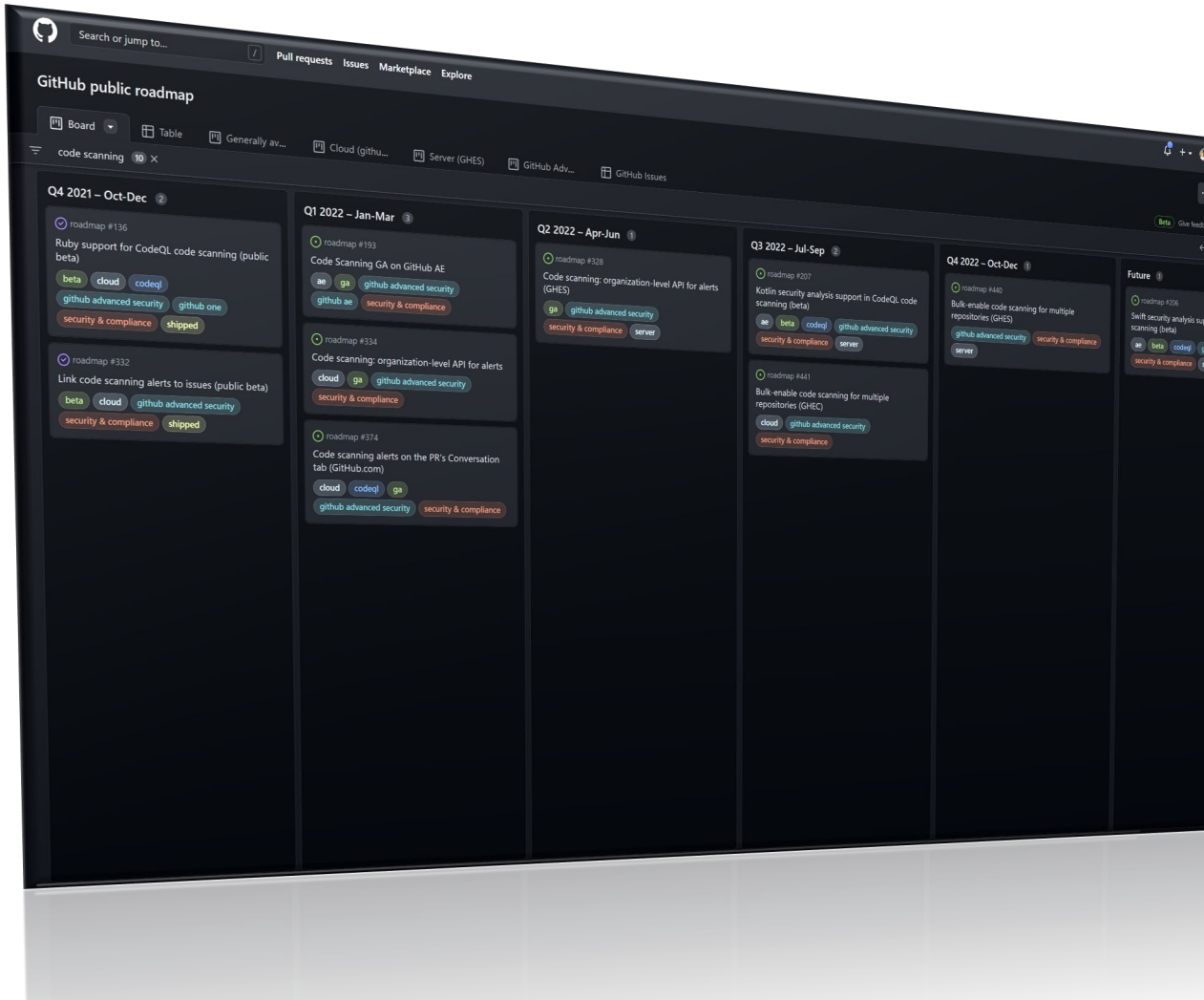
Let's see it in action

Conclusions

Is it perfect?

No, but…

- Low false positive rate
- Good all-around tool
- New languages are added regularly
- SARIF compatibility
- Integrated in the workflow



Recap: GitHub Code Scanning

- Extensible framework for code scanning
- Integrated within the developer workflow
- Backed by industry-leading CodeQL engine

- Customizable and Configurable

- Integrated with GitHub features

Worth Exploring

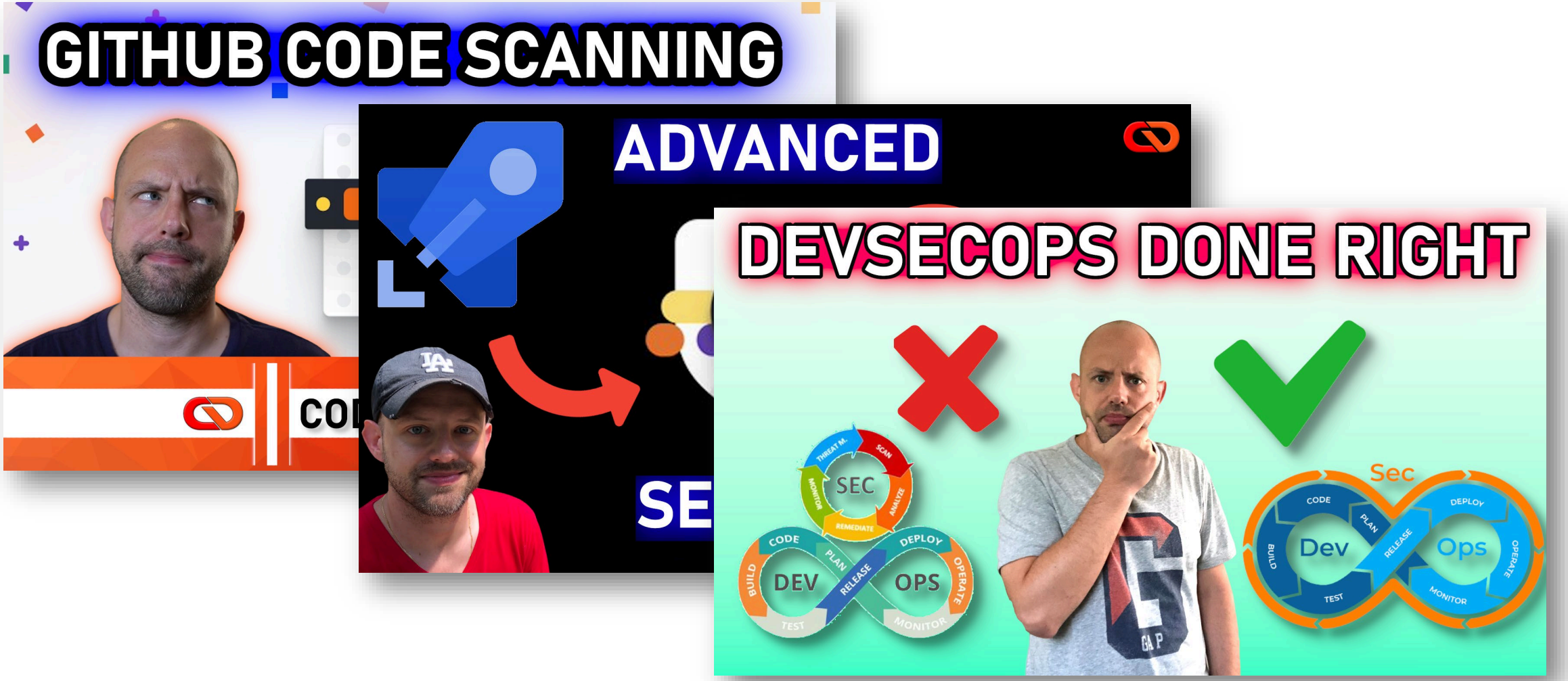
DEPENDENCY SCANNING

- Alerts and security updates for new vulnerabilities
- Integrated review when introducing new dependencies

SECRET SCANNING

- Scanning for leaked secrets in public and private repos
- Write custom patterns or rely on 100+ default ones
- Invalidate secrets/keys automatically

Videos


GITHUB CODE SCANNING
ADVANCED
DEVSECOPS DONE RIGHT
SEC
DEV
OPS
Sec
Dev
Ops

THANK YOU!

coderdave.io/join