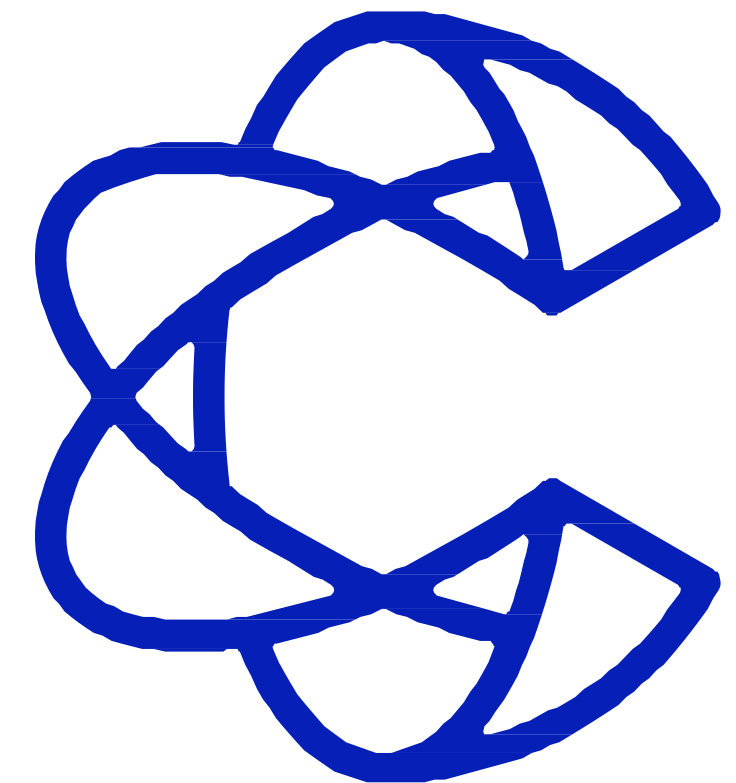


HOW TO HAVE VISIBILITY & SECURITY OF CICD ECOSYSTEM

Pramod Rana

@IAmVarchashva | github.com/varchashva



CODE BLUE 2025

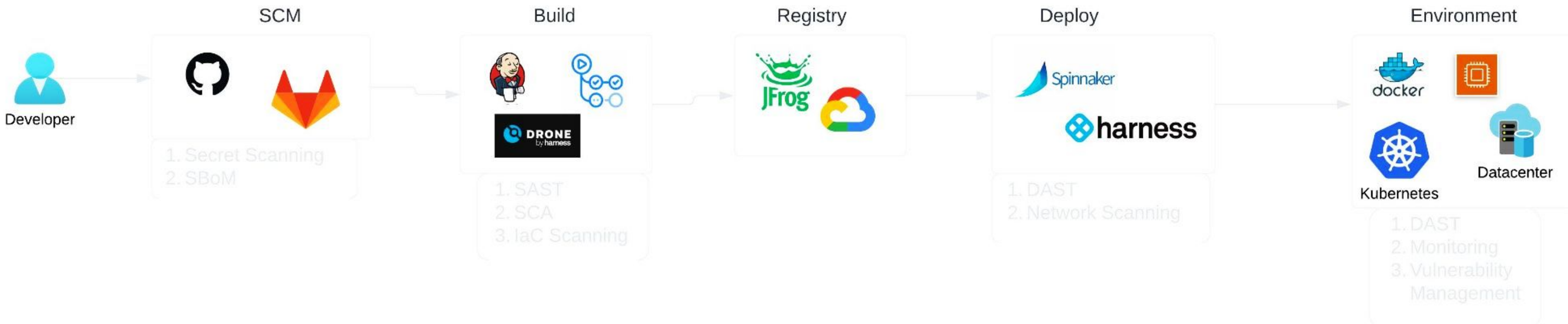
BECAUSE SECURITY MATTERS

ABOUT ME

- Sr. Manager - Application Security Assurance @Netskope
- Author of three open source projects:
 - [Omniscient](#) [*Let's Map Your Network*]: Graph-based asset management framework
 - [vPrioritizer](#) [*Art of Risk Prioritization*]: Risk prioritization framework
 - [CICDGuard](#) [*Security OF CICD*]: Orchestrating visibility & security of CICD ecosystem
- Speaker @BlackHat | Defcon | HITB | OWASPGlobalAppSec | Insomnihack | HackInParis | nullcon | HackMiami | DevOpsDays | CyberConAus | rootcon
- OWASP Pune Chapter Leader | OSCP

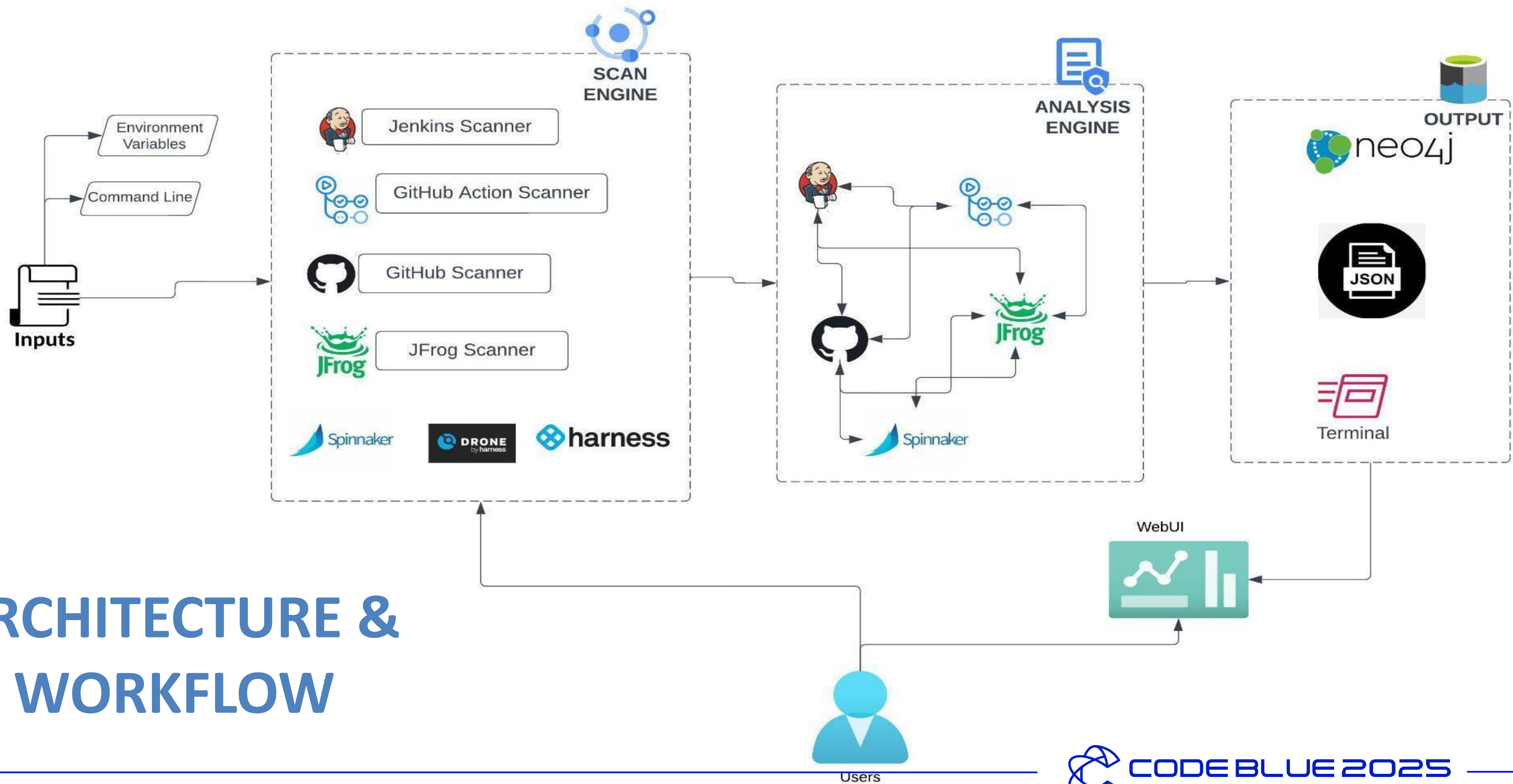
CONTEXT

- Secure the building blocks of CI/CD ecosystem. **#SecurityOfCI/CD**
- Compromise of one component impacts entire ecosystem
- Part of the problem is the lack of visibility into components & their configurations and interconnection between different technologies



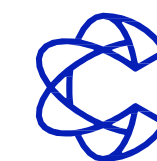
CICDGuard INTRODUCTION

- CICDGuard represents each component of building blocks into graph
- Identifies security misconfiguration in the implementation
- Identifies relationship between different technologies and thus impact of insecurity in one technology to others. For e.g.
 - Changes in a particular repo triggering a particular Jenkins job
 - Are we using vetted version of external GitHub Action
 - Do we have common users between Jenkins and JFrog and GitHub and so on...



ARCHITECTURE & WORKFLOW

DEMO



CODEBLUE2025
BECAUSE SECURITY MATTERS



[varchashva/CICDGuard](https://github.com/varchashva/CICDGuard)



@IAmVarchashva



varchashva@gmail.com
rana.miet@gmail.com

