



# APPSEC VULNERABILITY MANAGEMENT PIPELINES

# ACERCA DE MI...



/agustincelano



@agustincelano



/celagus



agustin.celano@baite.com.ar

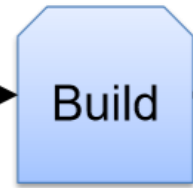
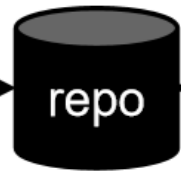
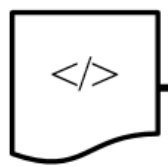


AGUSTIN CELANO

CISSP | PCAP | DSOE | DOL | CCNP



"lint" checks



INFRA / CONTAINER VULN SCAN

HARDENING + PATCH



Orchestrator



IAST

SCA

SAST

DAST

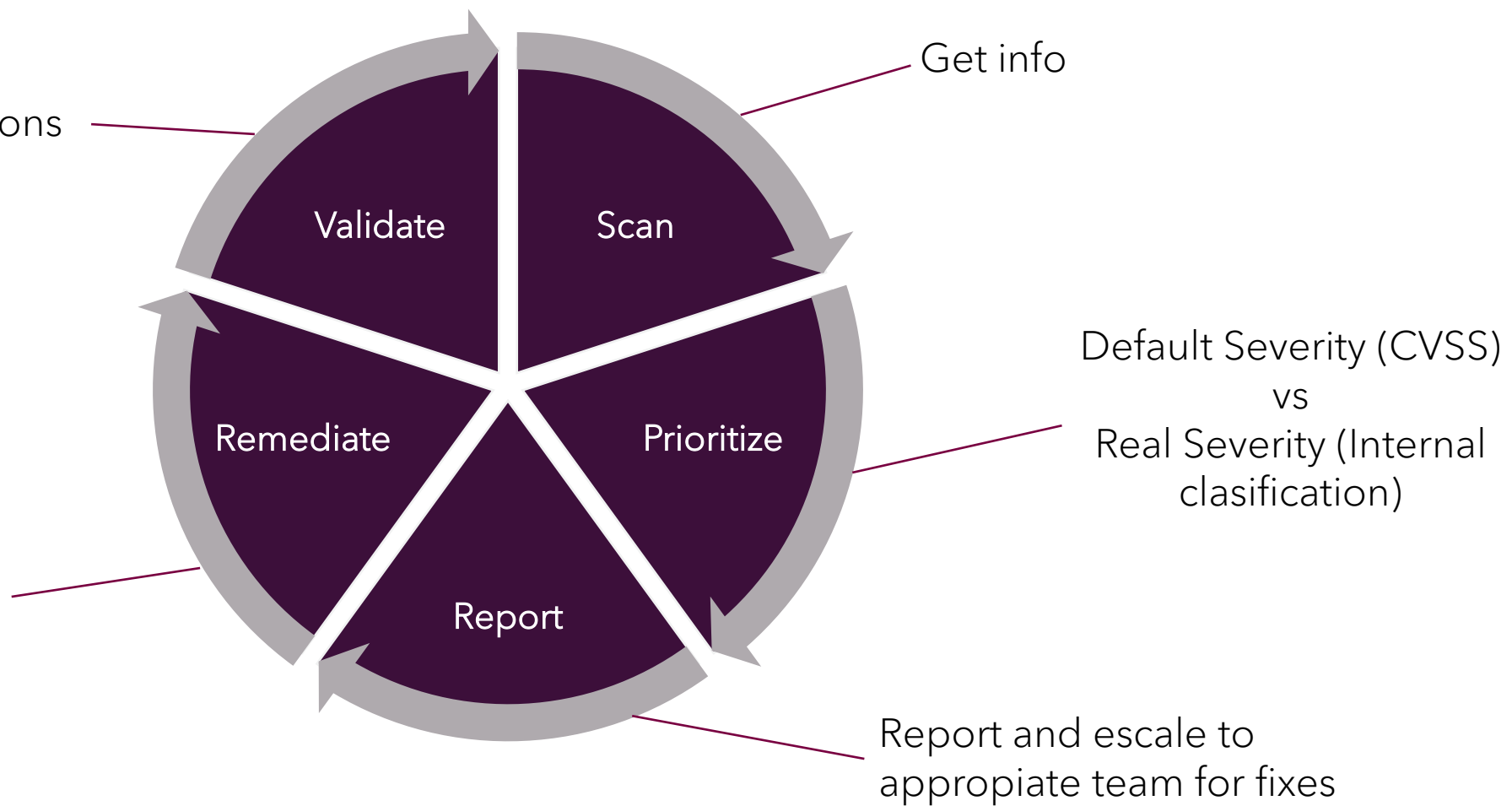
RASP

AUDIT

PENTEST

# DEVSECOPS APPSEC PIPELINE APPROACH

- Validate fixes
- Formalize risk management decisions
- Learn & Improve



# VULNERABILITY MANAGEMENT LIFE CYCLE

- Vulnerability must exist
- Exploitation must be feasible
- No compensatory controls

- Issue must be fixed before SLA expire or asset version is changed

Multiple VA tools

- Multiple origins
- Multiple formats
- Asynchronous run

False Positives

Prioritization / Ponderation

- Exploit available
- Publicated service
- Internal asset classification

Just in time remediation

- All vulns, actions and comments must be logged and be traceable

Tracking

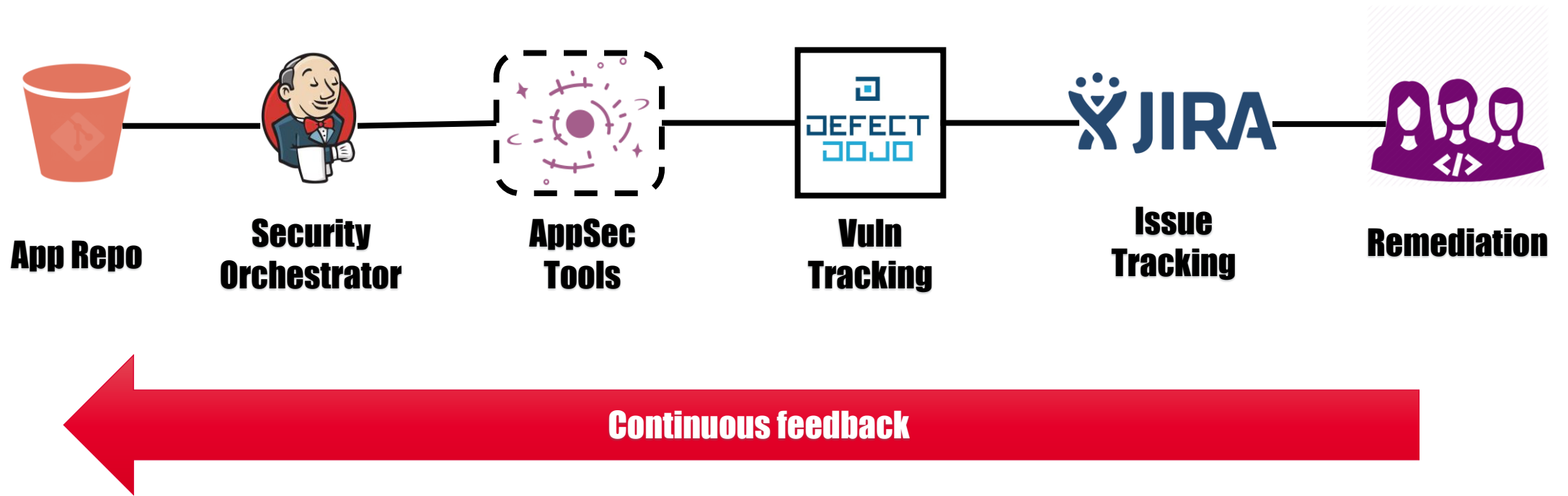
# COMMON VM PROCESS CHALLENGES

THIS IS DEVOPS, SO..

**BE AGILE,  
AUTOMATE!**

THAT IS VERY VERY IMPORTANT...





# APPSEC VM PIPELINE APPROACH

**DEMO  
TIME!**







*That's all Folks!*