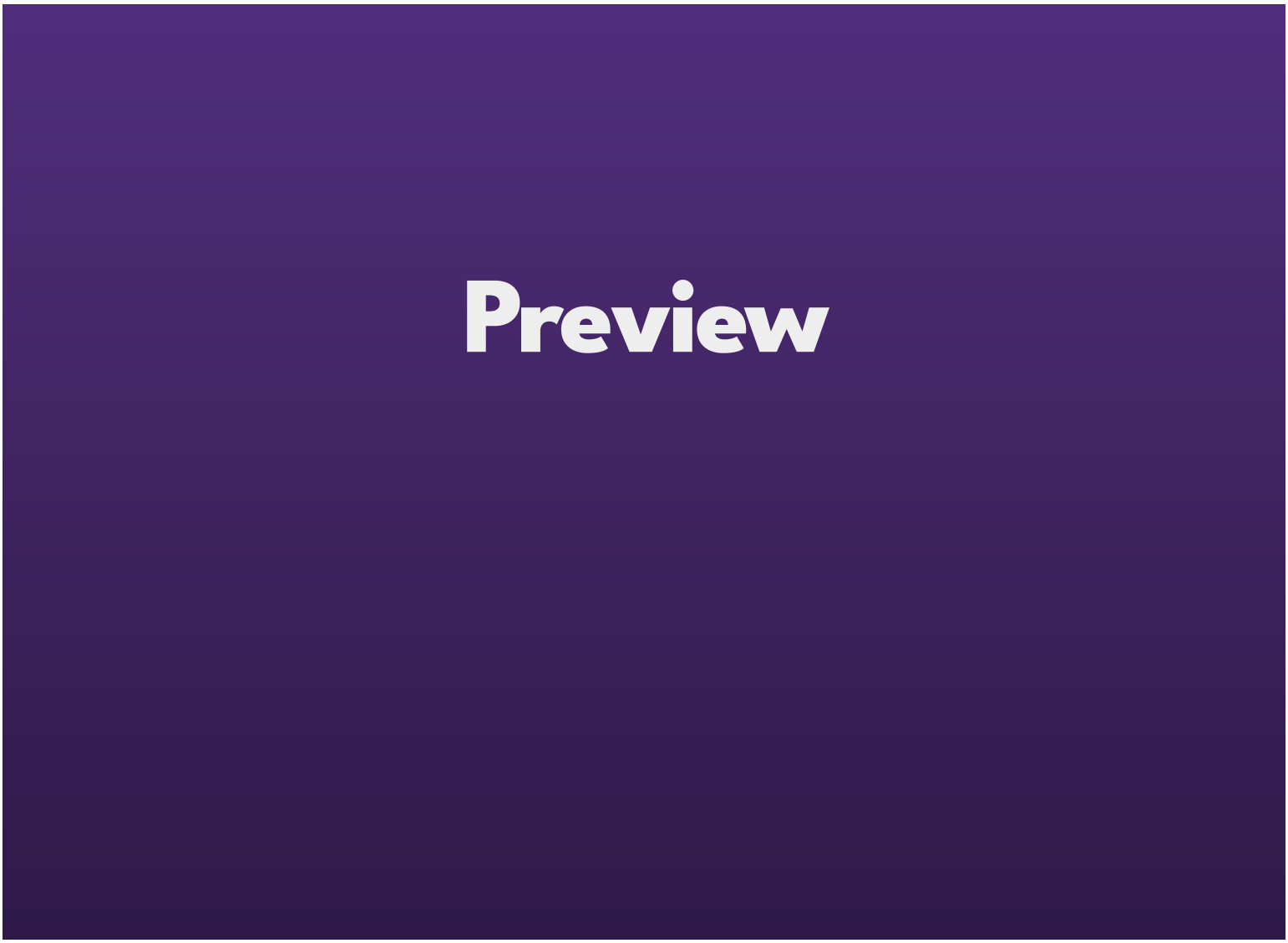
Clean Handoff

Giving devs the power and speed to deploy without the power of production

Evan Chiu, Software Engineering Director at Truist

Why does this matter?

- Separation of Duties
- Regulatory Concerns


Preview

Preview

- Empowering Dev Speed

Preview

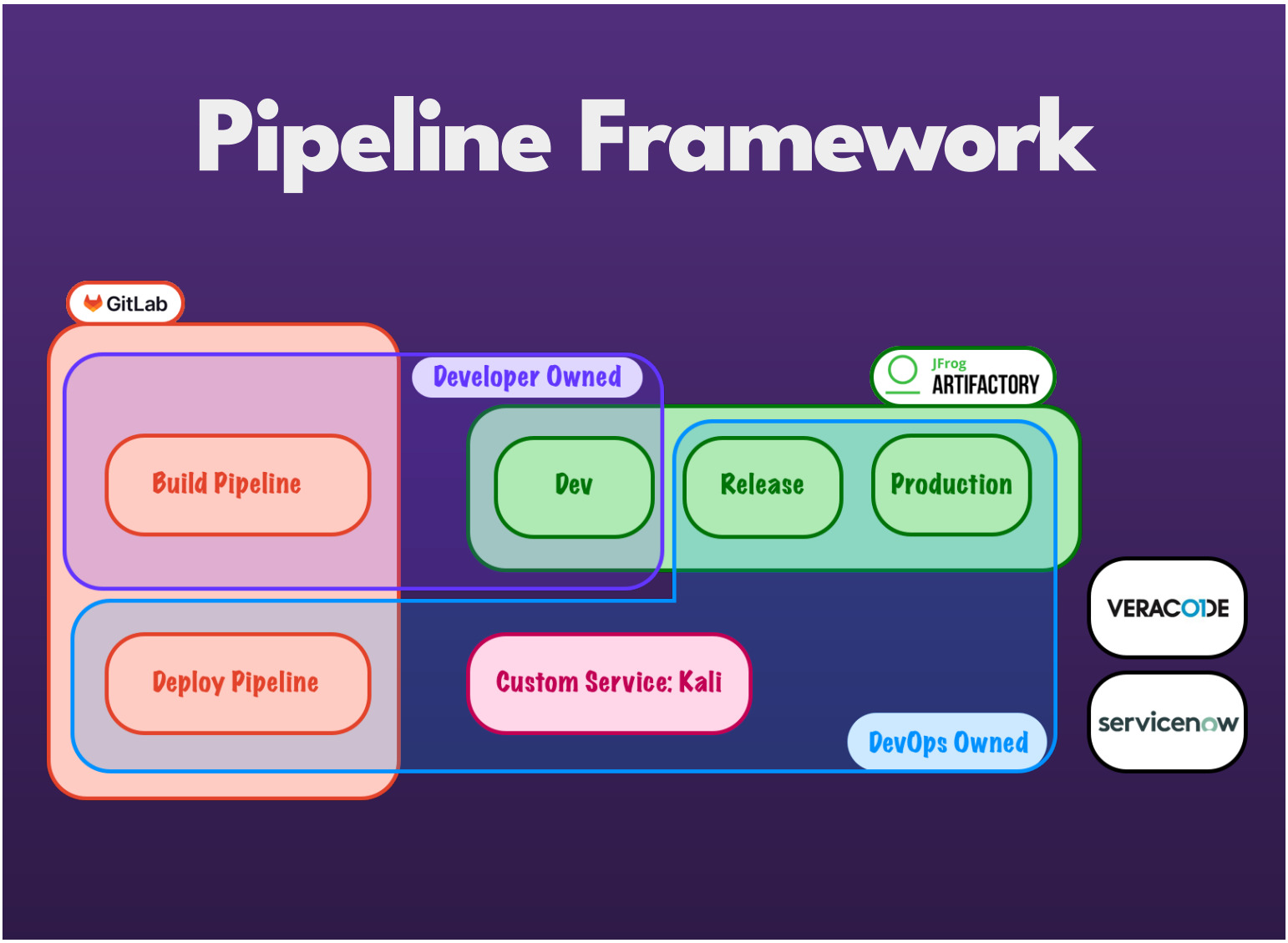
- Empowering Dev Speed
- Empowering Production Control

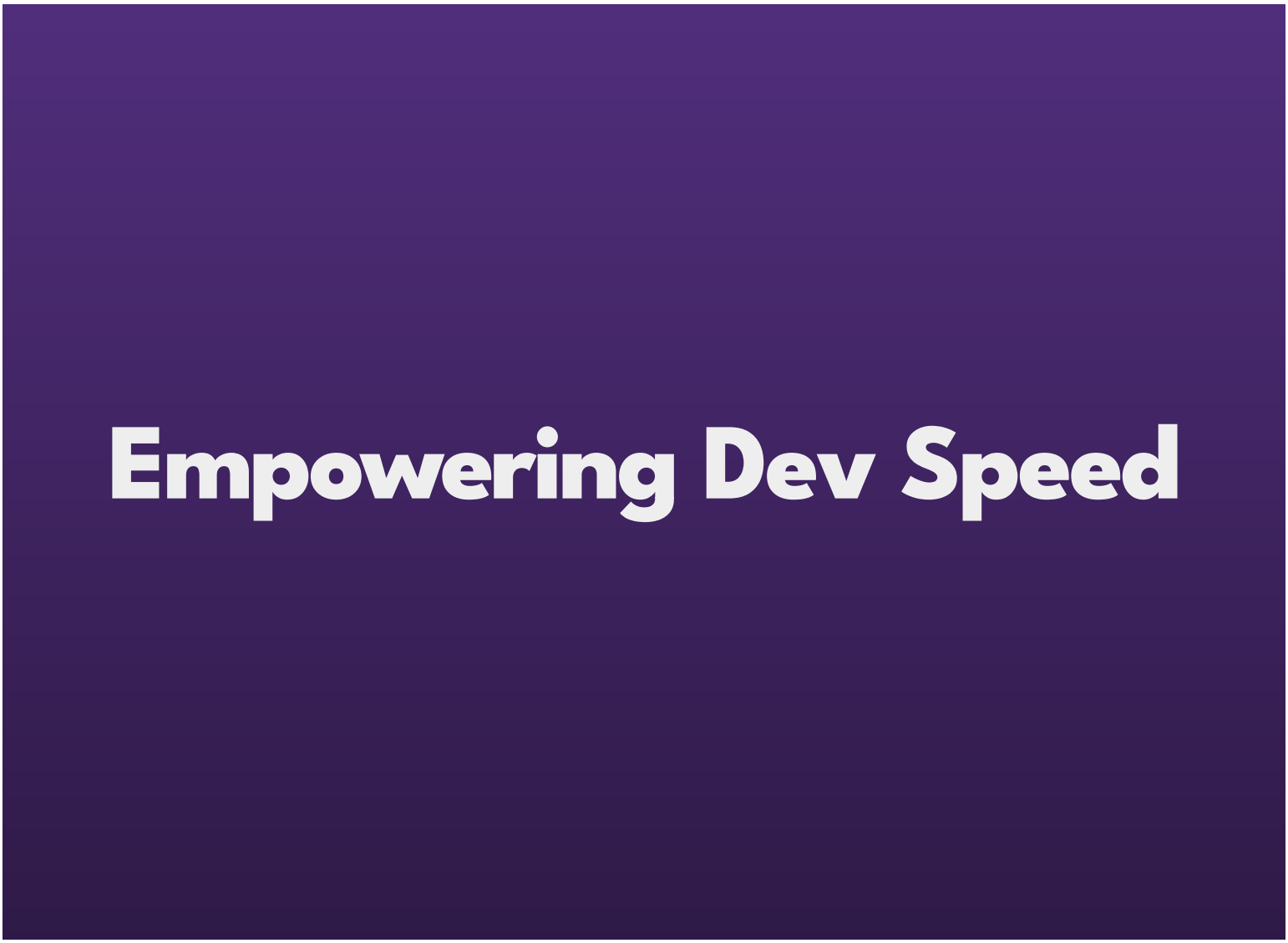
Preview

- Empowering Dev Speed
- Empowering Production Control
- Clean Handoff Techniques

Preview

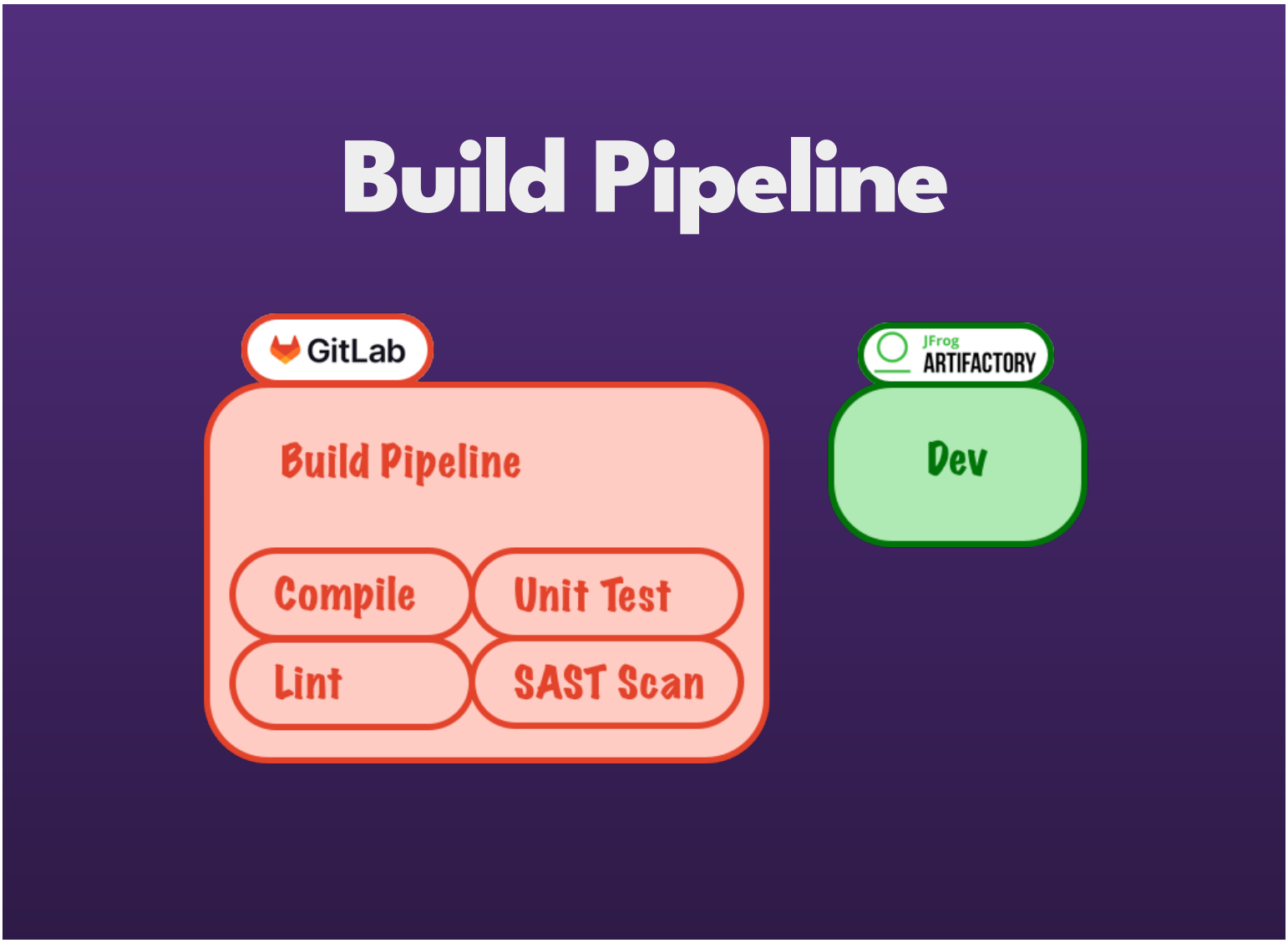
- Empowering Dev Speed
- Empowering Production Control
- Clean Handoff Techniques
- Custom Service: Kali


Pipeline Framework
GitLab
Developer Owned
JFrog ARTIFACTORY
Build Pipeline
Dev
Release
Production
VERACODE
Deploy Pipeline
Custom Service: Kali
servicenow
DevOps Owned


Empowering Dev Speed

Devs Own Builds

- Everything is an artifact
- Build once, run everywhere


Build Pipeline
GitLab
Build Pipeline
Compile
Unit Test
Lint
SAST Scan
JFrog
ARTIFACTORY
Dev

Templates

- GitLab pipelines as Code
- Templates for everything

```
build-publish:
  script:
    - yarn install
    - yarn build
    - yarn pack
    - curl -T $ARTIFACT https://artifactory/${NAME}-${VERSIC
```

Pre-merge testing

- Compile
- Unit test
- Linting
- Sandbox SAST Scan

Branch Deploys

- Allows deployment of unreviewed code in a limited environment

Security-injected Code Review

Security reviews all IAM role and policy changes at merge request time


Empowering Production
Control

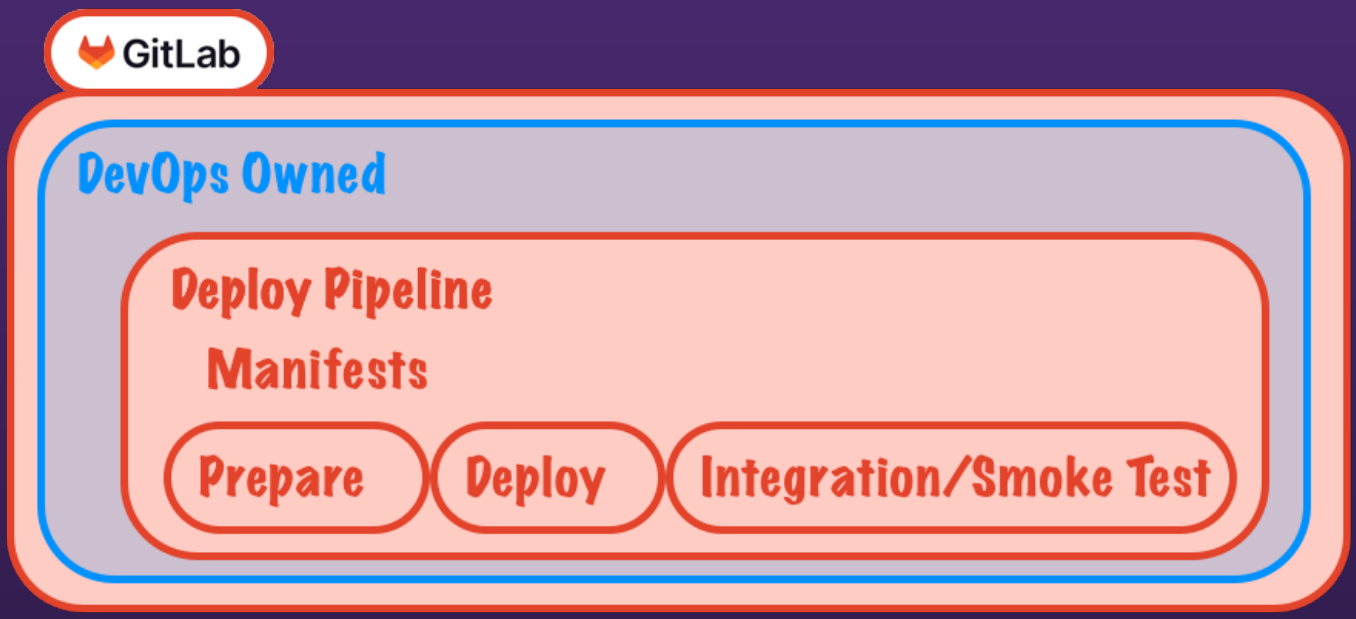
Deploy Projects

- GitLab pipelines as code, using templates
- Manifest files identify the versions of artifacts needed for deployment

Manifest

```
{
  "artifacts": [
    {
      "name": "api-lambda",
      "type": "lambda",
      "version": "1.2.3",
      "location": "https://artifactory/lambda-v1.2.3.zip",
      "commit": "https://gitlab/lambda-project/f15d763",
    },
    {
      "name": "app-infrastructure-as-code",
      "type": "terraform",
      "version": "1.2.5",
      "location": "https://artifactory/terraform-v1.2.5.zip",
      "commit": "https://gitlab/infra-project/8f5a435",
    }
```

Deploy Project Diagram



ServiceNow Validation

- Call ServiceNow to ensure change record is ready

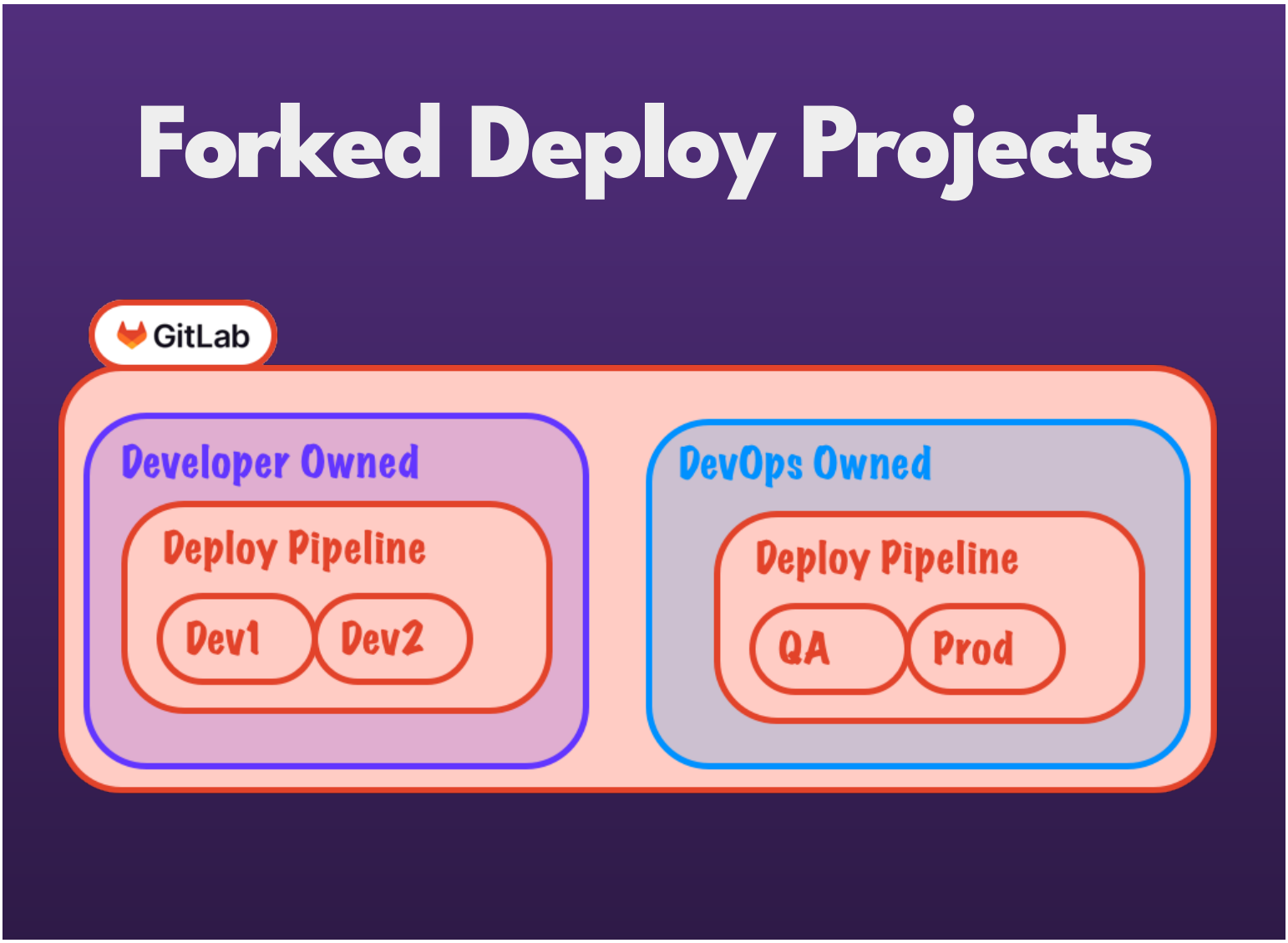

Clean Handoff via DevOps

DevOps Dojo

- Walkthrough every part of building an application at Truist
- Available in the primary programming languages our teams use

Forked Deploy Projects

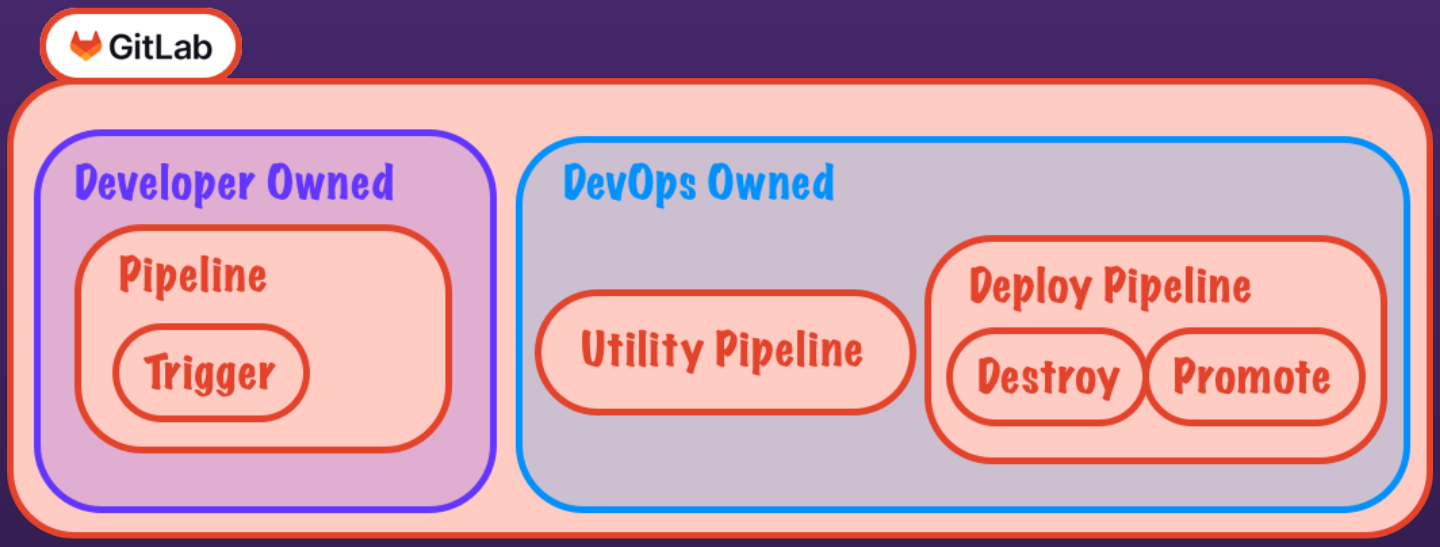
Fork the deploy project to allow dev control of lower environments


Forked Deploy Projects
GitLab
Developer Owned
Deploy Pipeline
Dev1
Dev2
DevOps Owned
Deploy Pipeline
QA
Prod

GitLab Utility Pipelines

- Pipelines as an API
- This technique allows us to give dev teams a trigger token to run our pipeline, allowing us to fully separate access control

GitLab Utility Pipelines



Utility Pipeline Trigger

```
destroy-dev1:
  script:
    - >
      curl --request POST
      --form token=$TRIGGER_TOKEN
      --form ref=main
      --form "variables[ENV]=dev1"
      https://gitlab/api/v4/projects/$DEPLOY_ID/trigger/pipeline
```

Automated Change Tickets

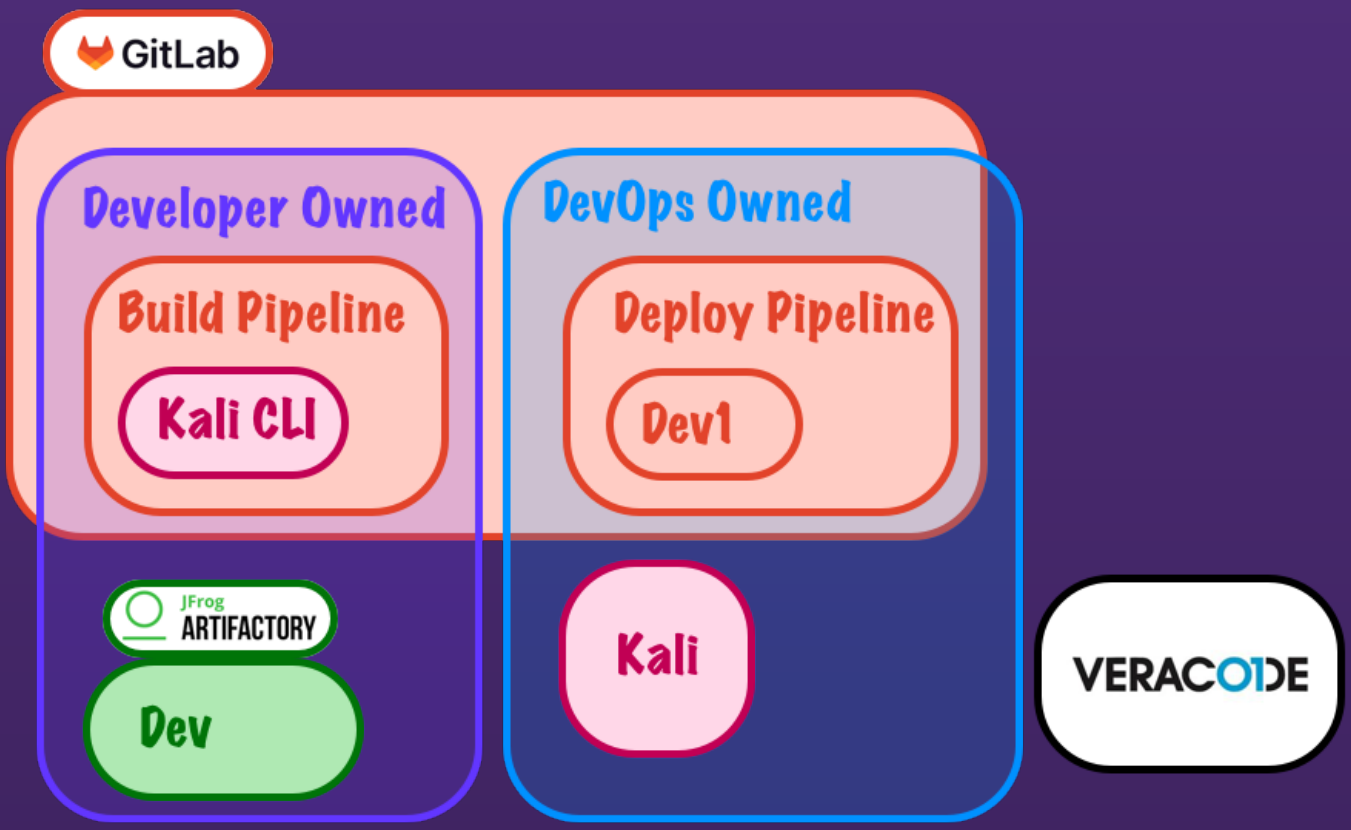
- Automated change ticket creation
- Automated evidence collection


Custom Service: Kali

Kali Build integration

Build pipelines call Kali CLI to push their artifacts into Artifactory, then call the Kali service to inform it of the new artifact

Kali Build Diagram



Kali Compliance

- Kali kicks off long-running SAST scans in the background
- Kali integration in deploy pipelines confirms scan success

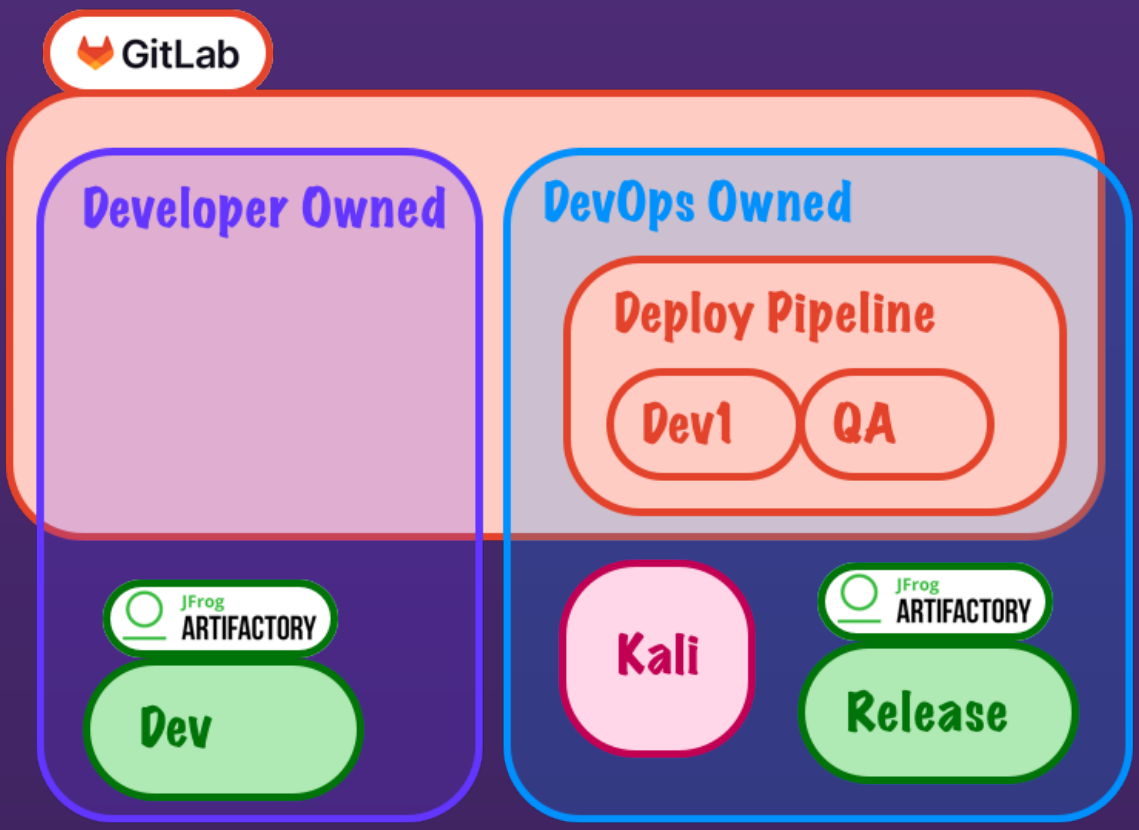
Kali Deploy Integration

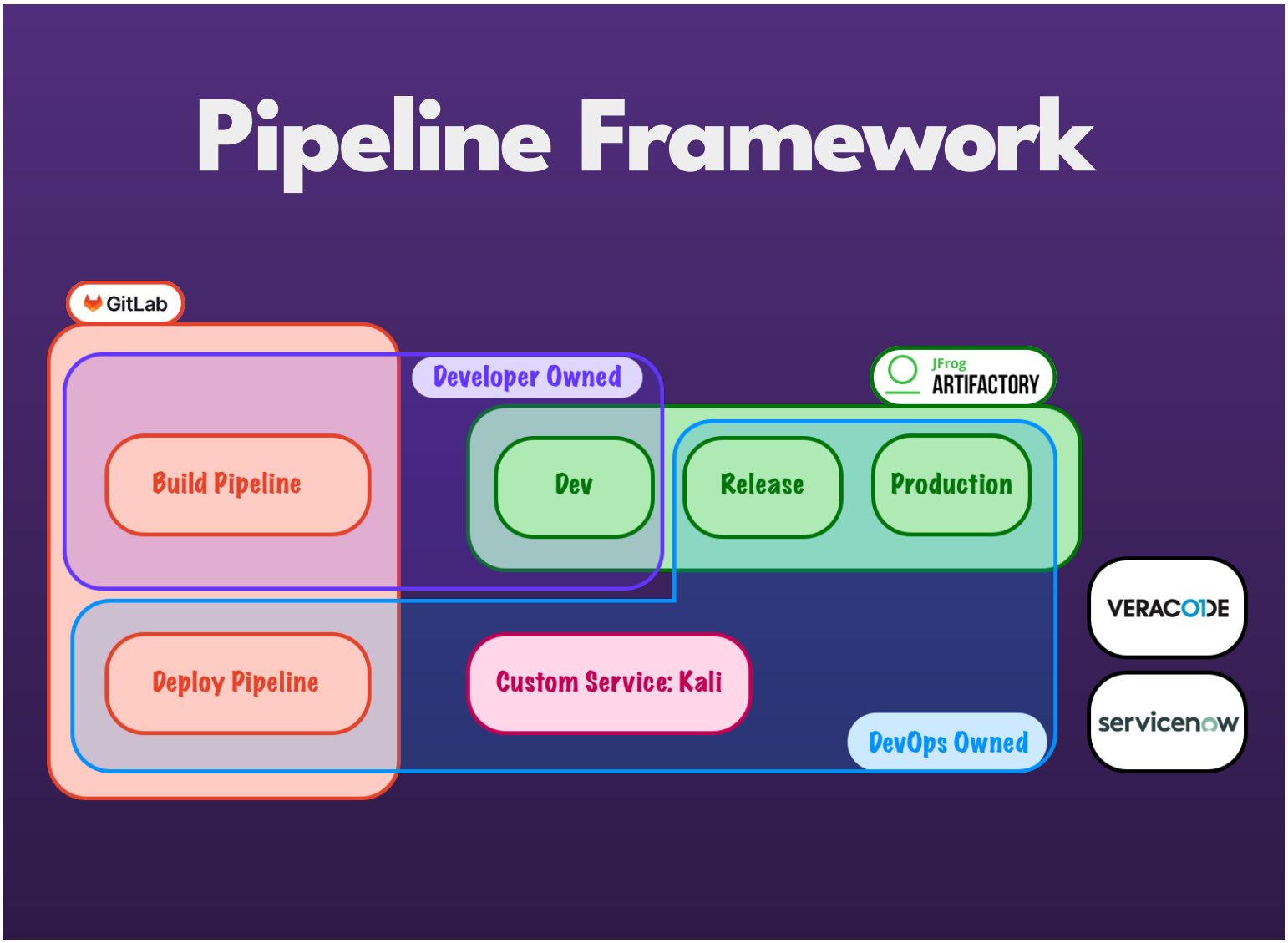
Kali tracks every version of every artifact, when a new version comes in, it updates the manifest in the deploy project

Kali Promotion

- Kali promotes artifacts through the environments
- Allows increasing the control requirements for each environment
- Copies artifacts between the Artifactory repositories (necessary for retention)

Kali Promote Diagram




Pipeline Framework
GitLab
Developer Owned
JFrog ARTIFACTORY
Build Pipeline
Dev
Release
Production
VERACODE
Deploy Pipeline
Custom Service: Kali
servicenow
DevOps Owned

Summary

Summary

- Dev Ownership

Summary

- Dev Ownership
- Everything is an artifact

Summary

- Dev Ownership
- Everything is an artifact
- Utility Pipelines

Summary

- Dev Ownership
- Everything is an artifact
- Utility Pipelines
- Automated ticketing

Summary

- Dev Ownership
- Everything is an artifact
- Utility Pipelines
- Automated ticketing
- Custom Service

Summary

- Dev Ownership
- Everything is an artifact
- Utility Pipelines
- Automated ticketing
- Custom Service

Evan Chiu, evanchiu.com
careers.truist.com