GIT AND GET GOING

Sanjay Shrestha
Principal Detection Engineer, Bayer

Raanan Dagan
Principal Sales Engineer, Cribl

AGENDA

CRIBL @ BAYER

GITOPS OVERVIEW

GITOPS LESSON LEARNED

DEMO

BEST PRACTICES

Q&A

CRIBL @ BAYER

2012
Splunk introduced

2018
Monsanto → Bayer

2020
80 GB/day → Over 13 TB/day

2021
On-Prem → Splunk Cloud

2021
Splunk Operational Cost

2022
Splunk Dynamic Data Active Archive* Cost

*DDAA

CRIBL @ BAYER

2022

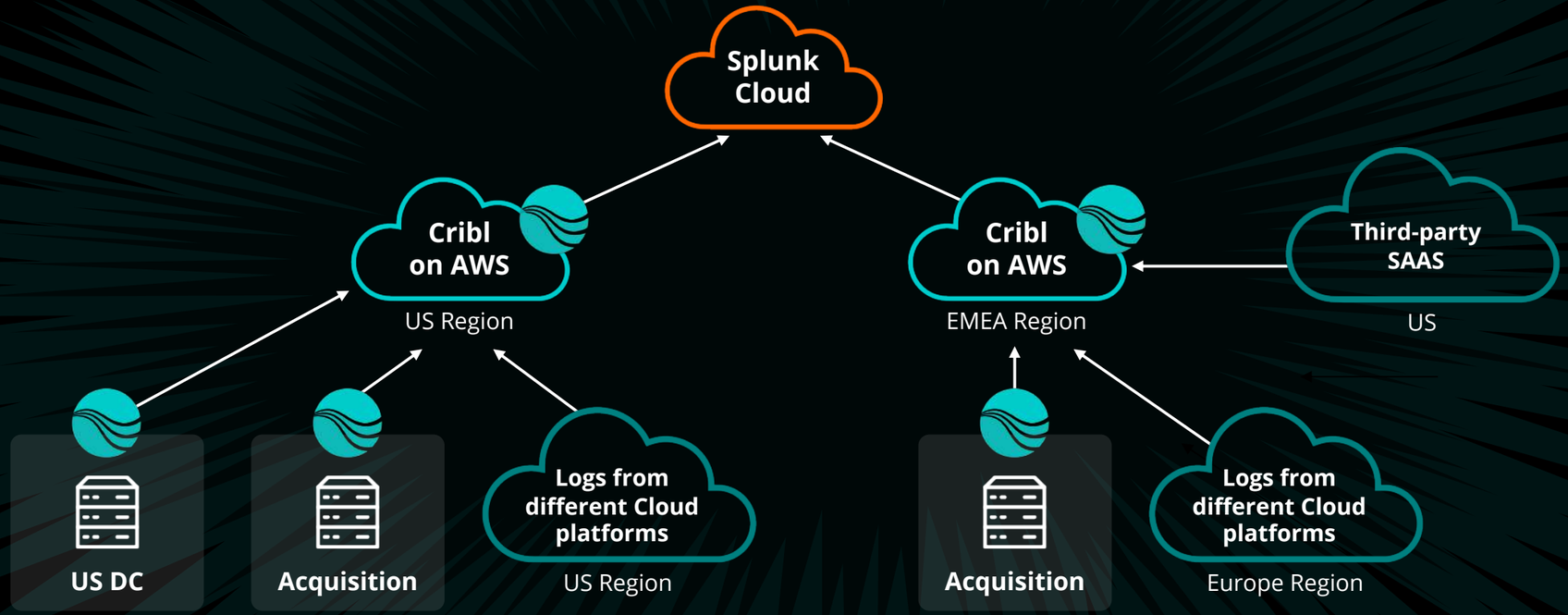
Cribl introduced last year

- Cribl reduced Splunk Operational Cost by **30%**
- Cribl reduced Splunk DDAA Cost by **70%**
- **Leverage** Cribl to Cribl Integration
- Data Management and Processing **efficiency**
- **Flexibility** to use multiple SIEM solutions

CRIBLCON! 2023

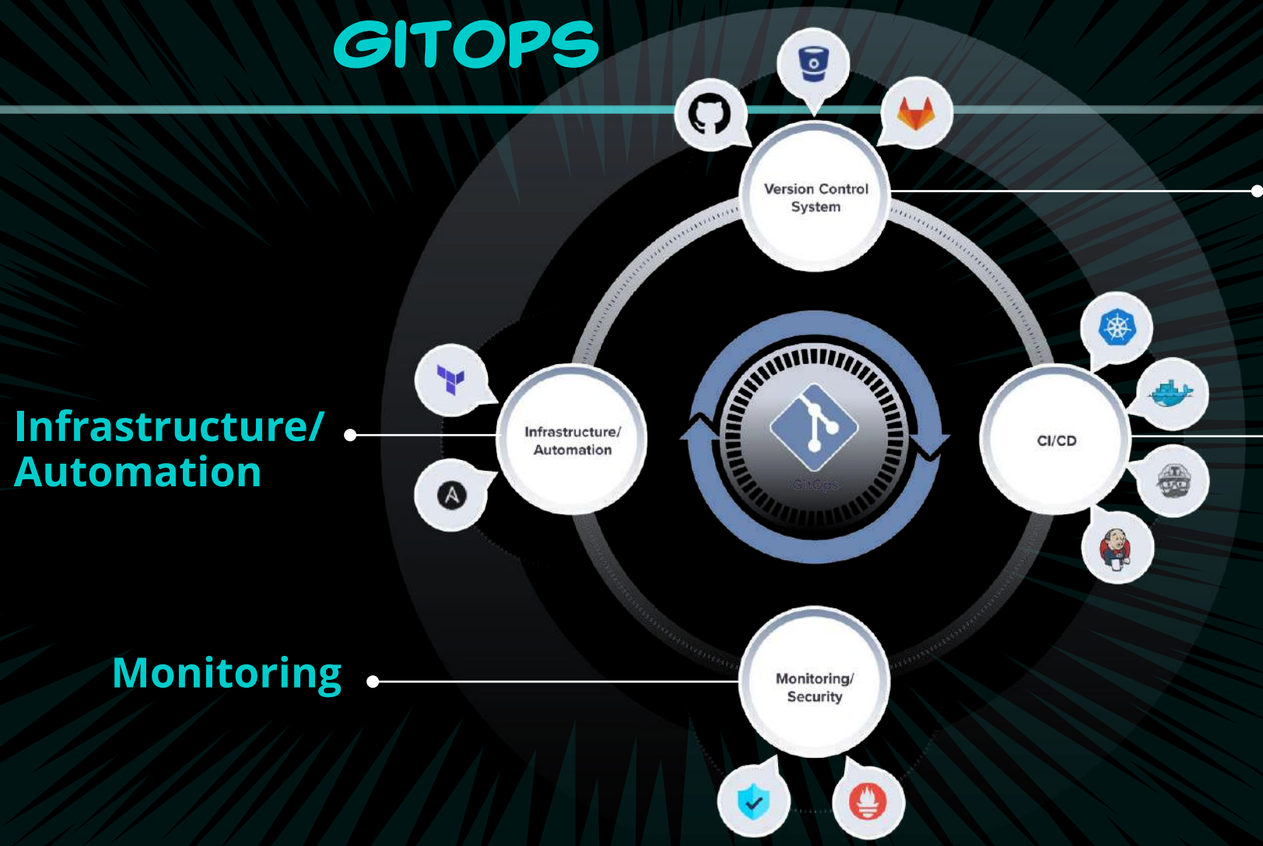
BAYER

CRIBL @ BAYER


Splunk Cloud
Cribl on AWS
US Region
Cribl on AWS
EMEA Region
Third-party SAAS
US
US DC
Acquisition
Logs from different Cloud platforms
US Region
Acquisition
Logs from different Cloud platforms
Europe Region

GitOps is **an operational model** that applies **DevOps** (development and ops/operations) practices like:

- Version Control
- CI/CD
- Monitoring
- Infrastructure/ Automation



Version Control

- GitHub, GitLab, Bitbucket

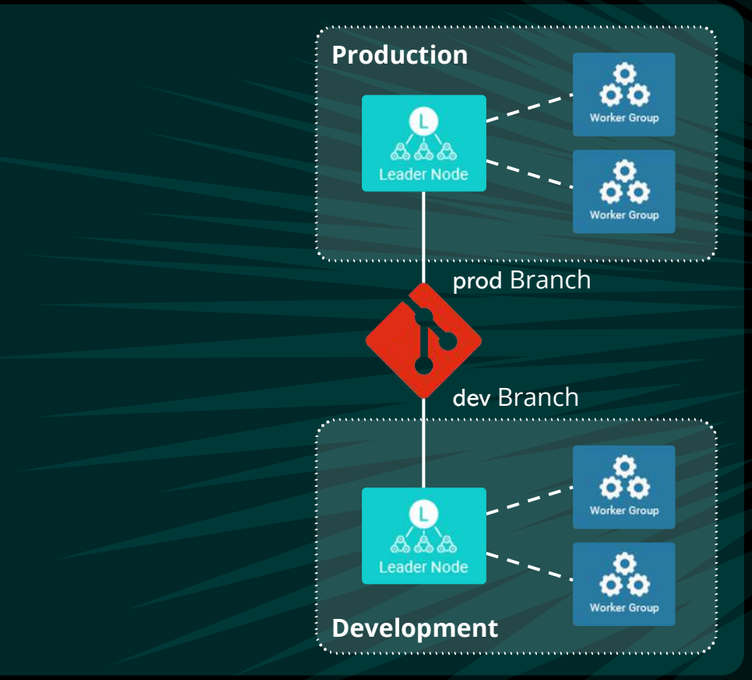
CI/CD
(Continuous Integration/ Continuous Delivery

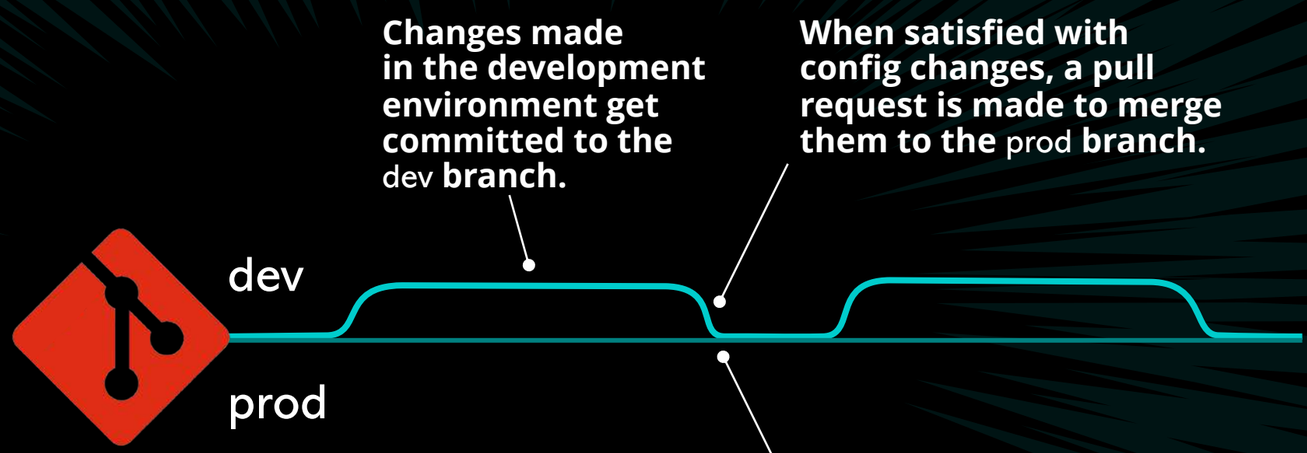
- Docker, Jenkins

Infrastructure/ Automation

Monitoring

CRIBL WITH GITOPS PRODUCT CAPABILITIES

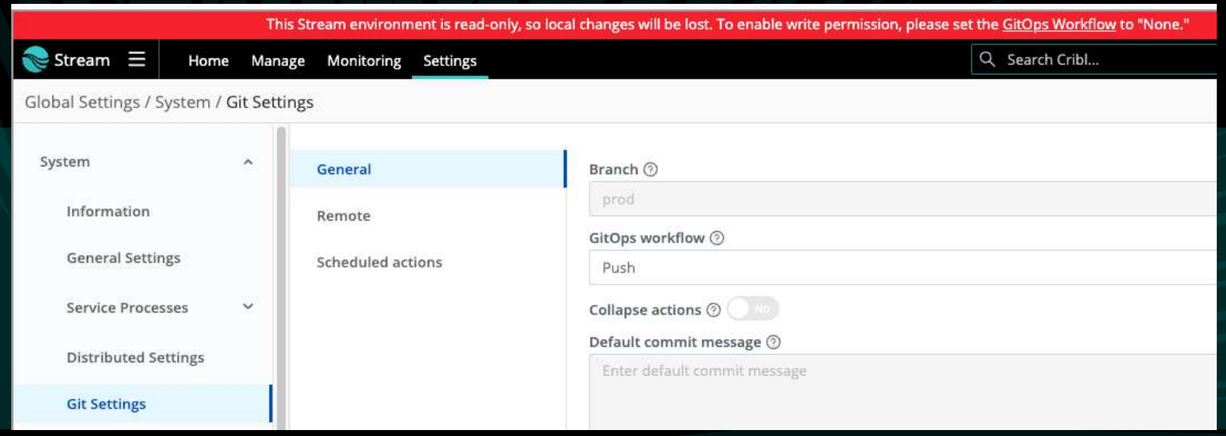




CRIBL WITH GITOPS PRODUCT CAPABILITIES

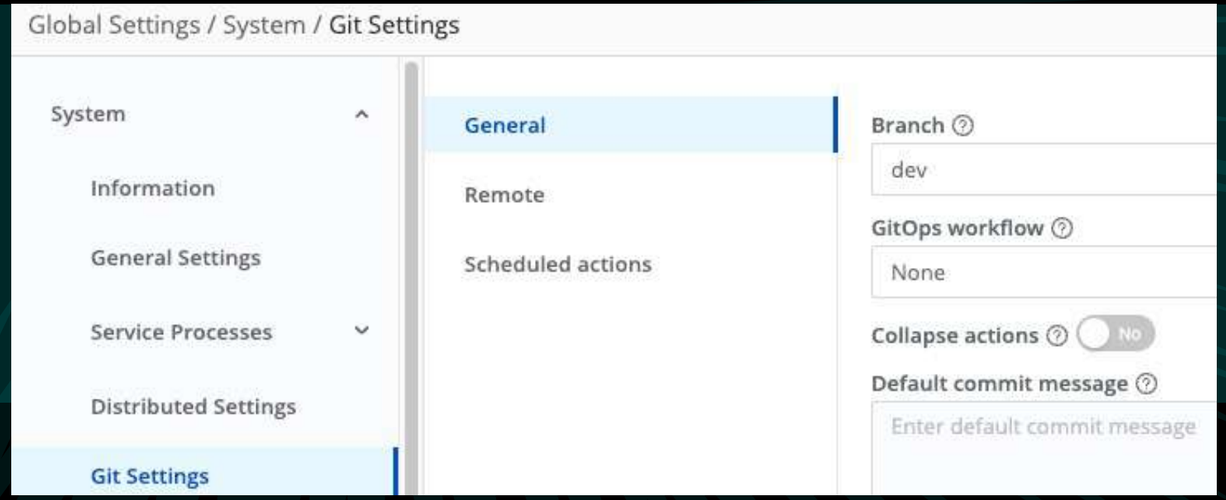
Production

- GitOps workflow = Push
- Read Only
- Get data from Git



Development

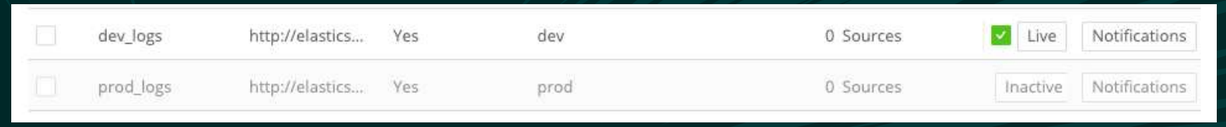
- GitOps workflow = None
- Read and Write
- Send data to Git



CRIBL WITH GITOPS PRODUCT CAPABILITIES

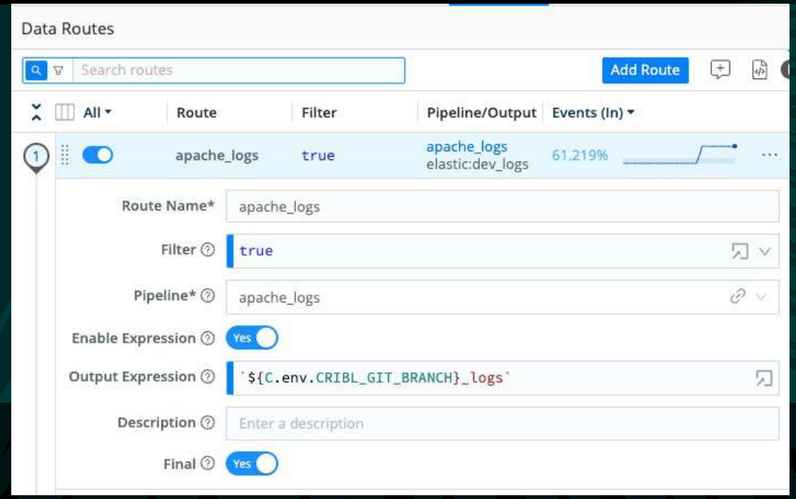
Sources and Destinations

- Environment to understand bucket
- Live or Inactive

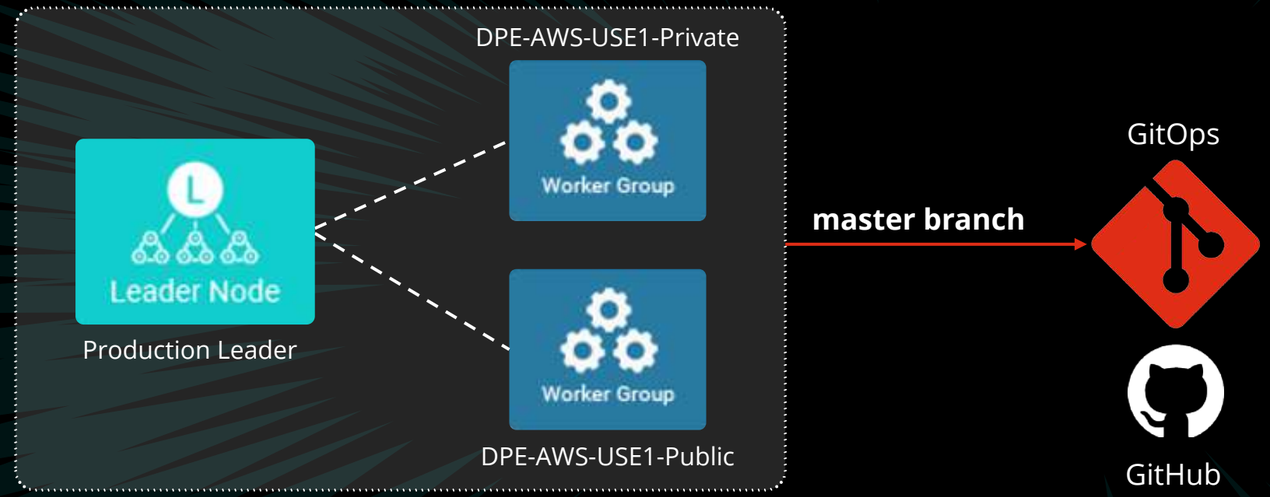


Routes

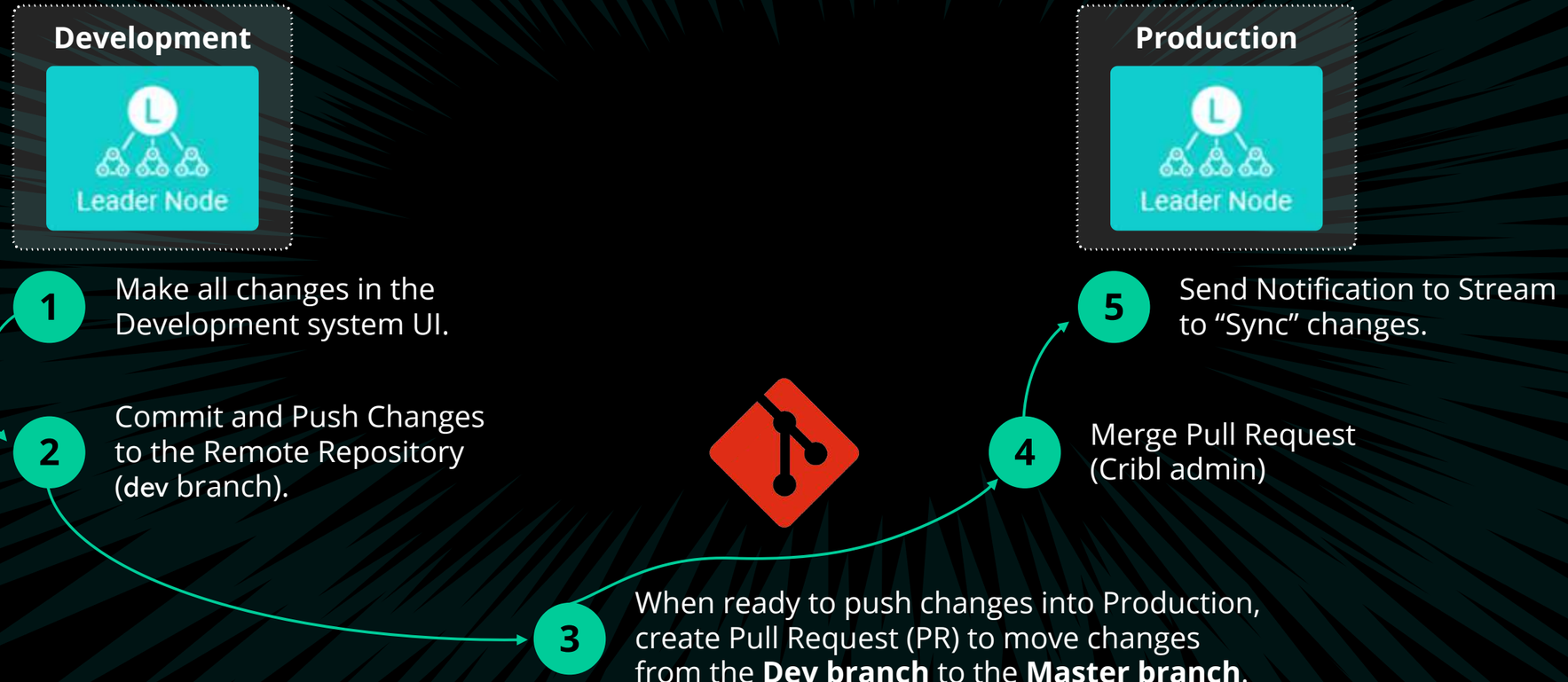
- Output Expression to understand bucket



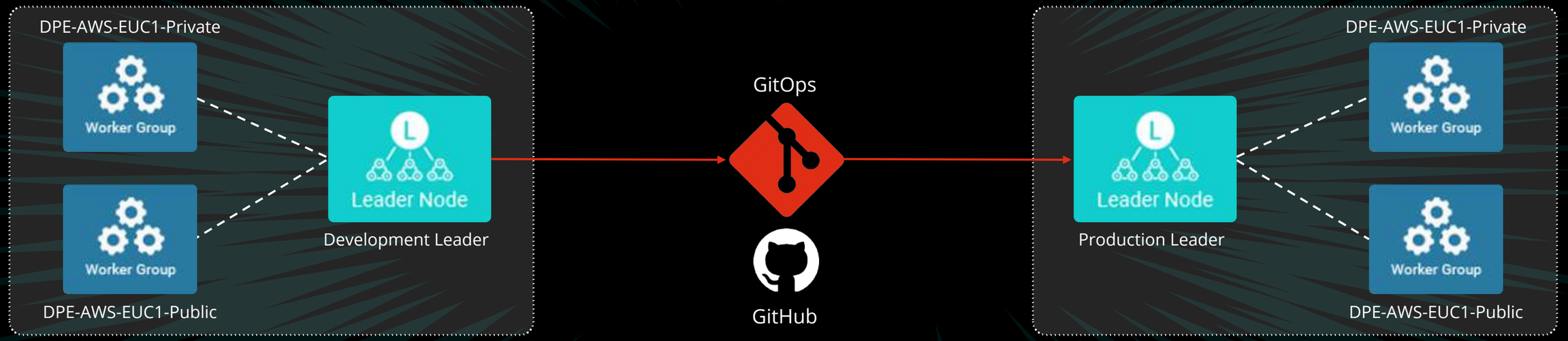
CRIBL WITH GITOPS PRODUCT CAPABILITIES



GITOPS—FUTURE MODE OF OPERATION (FMO)



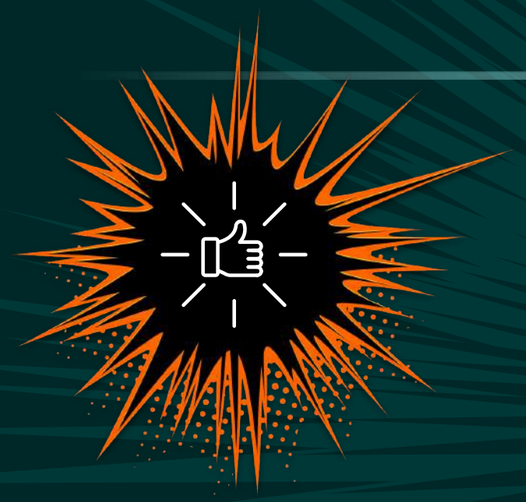
GITOPS—FUTURE MODE OF OPERATION (FMO)



Development Environment
dev branch

Production Environment
master branch

BEST PRACTICES



BEST PRACTICES

- Create private repository.
- Grant access to users as per need basis.
- git .ignore
- To use as backup to restore environment.
- Use declarative comments.
- Choose branches over repositories.
- Worker/Global Commit and Deploy
- Continuous Push and Commit

REFERENCES

REFERENCES

https://www.atlassian.com/git/tutorials/what-is-git

https://cribl.io/blog/cribl-and-gitops/

https://docs.cribl.io/stream/gitops/


CRIBLCON!
2023