



## GIT AND GET GOING

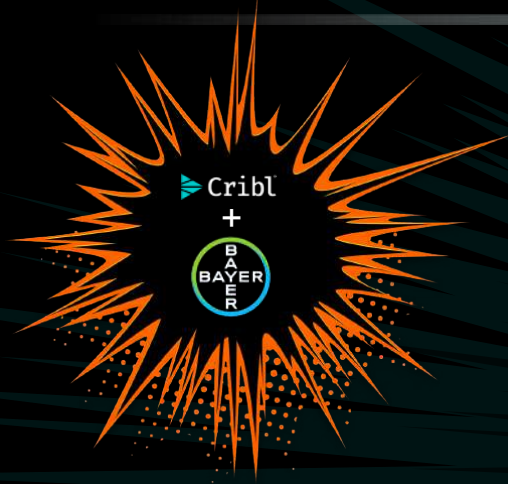
**Sanjay Shrestha**

Principal Detection  
Engineer, Bayer

**Raanan Dagan**

Principal Sales  
Engineer, Cribl

# AGENDA



CRIBL @  
BAYER



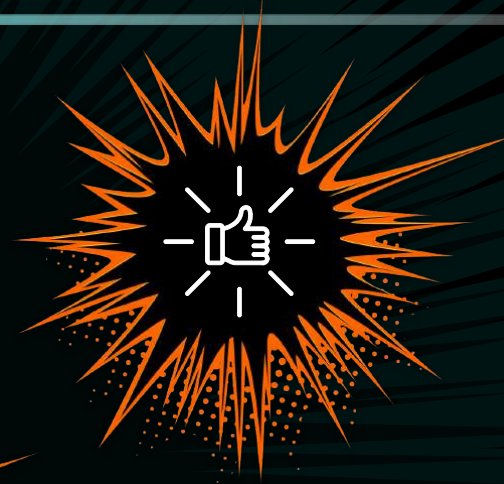
GITOPS  
OVERVIEW



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

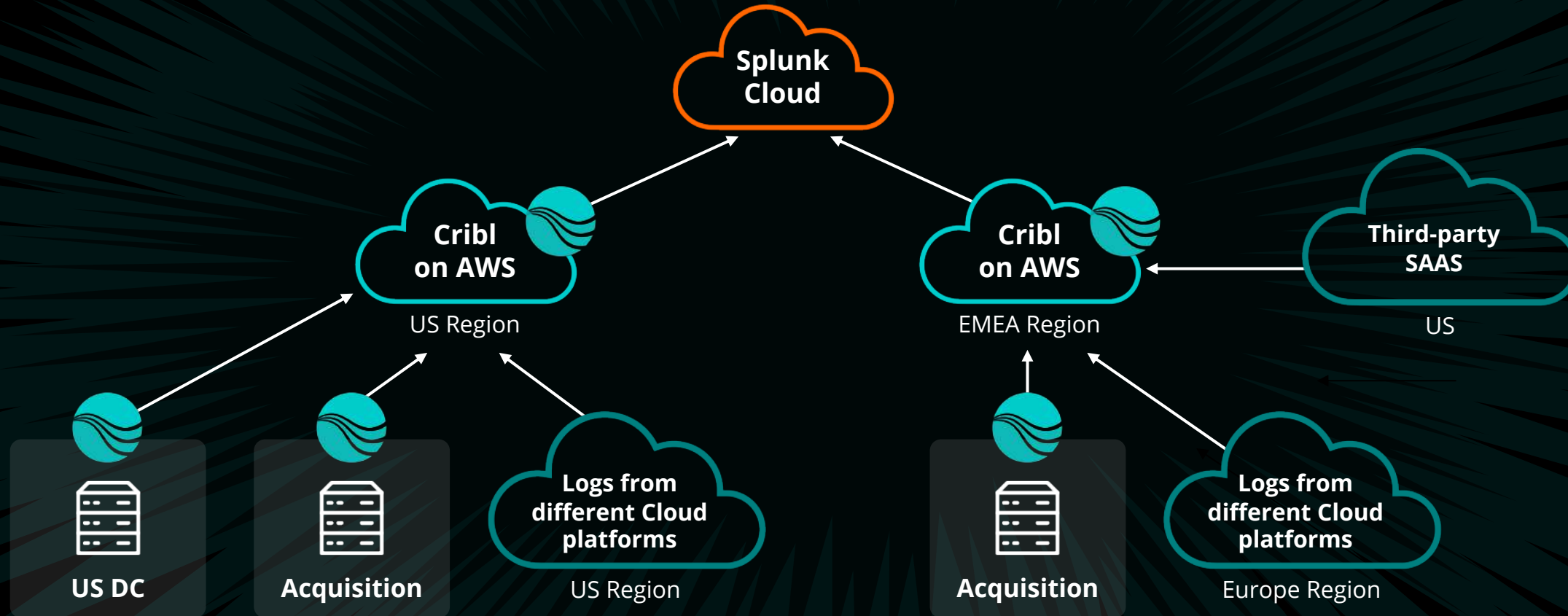
2022

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

# CRIBL @ BAYER





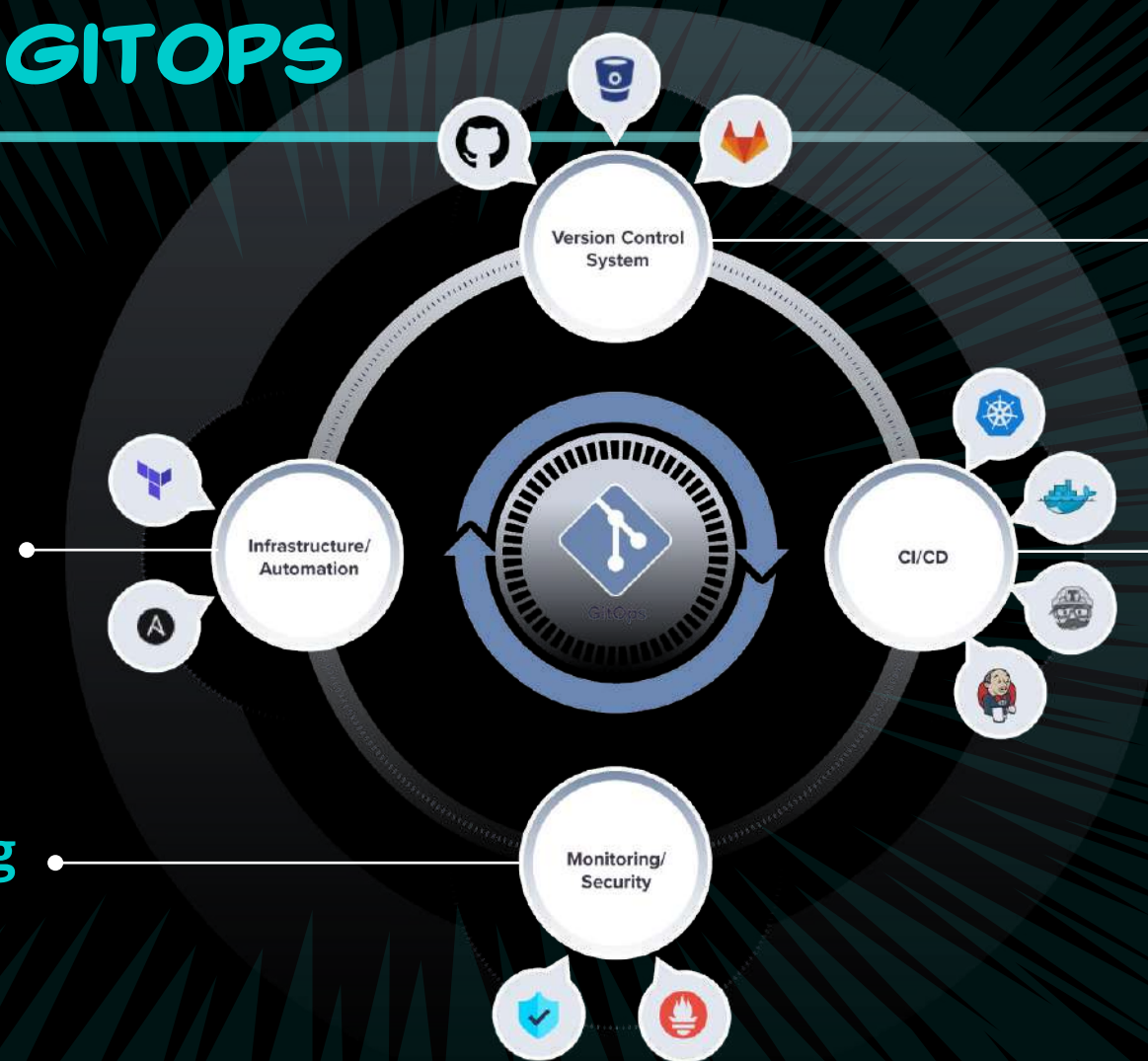
# GITOPS

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

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

**Infrastructure/ Automation**

**Monitoring**



**Version Control**

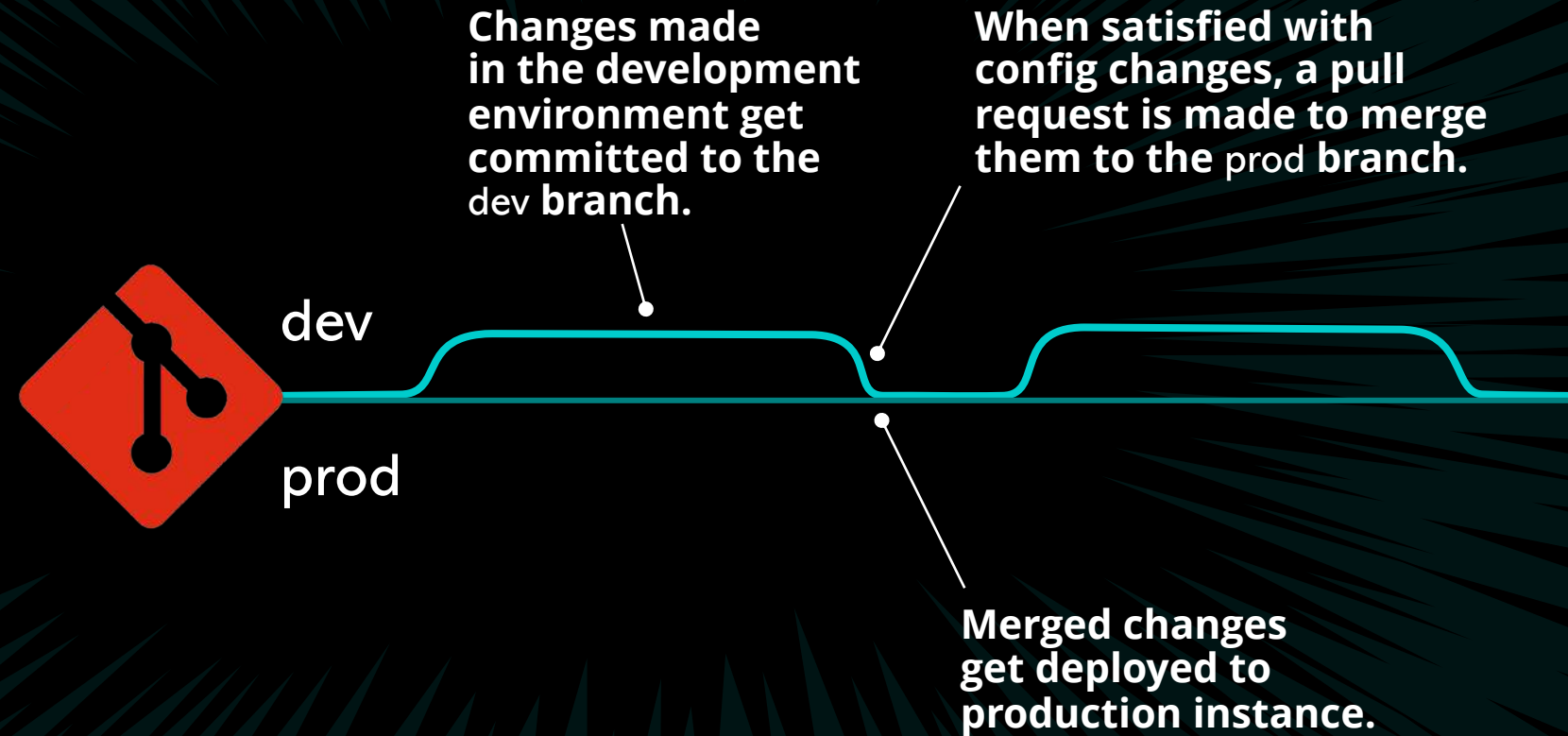
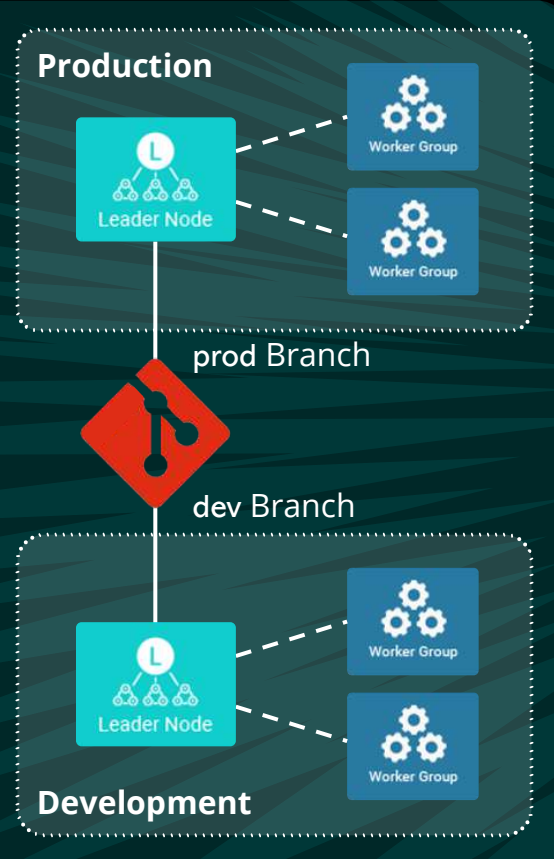
- GitHub, GitLab, Bitbucket

**CI/CD**

(Continuous Integration/ Continuous Delivery)

- Docker, Jenkins

# 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

This Stream environment is read-only, so local changes will be lost. To enable write permission, please set the GitOps Workflow to "None."

Stream Home Manage Monitoring Settings Search Cribl...

Global Settings / System / Git Settings

System ^

- Information
- General Settings
- Service Processes v
- Distributed Settings
- Git Settings

General

- Remote
- Scheduled actions

Branch ?

prod

GitOps workflow ?

Push

Collapse actions ?  No

Default commit message ?

Enter default commit message

Global Settings / System / Git Settings

System ^

- Information
- General Settings
- Service Processes v
- Distributed Settings
- Git Settings

General

- Remote
- Scheduled actions

Branch ?

dev

GitOps workflow ?

None

Collapse actions ?  No

Default commit message ?

Enter default commit message



# CRIBL WITH GITOPS PRODUCT CAPABILITIES



## Sources and Destinations

- Environment to understand bucket
- Live or Inactive

<input type="checkbox"/>	dev_logs	http://elastics...	Yes	dev	0 Sources	<input checked="" type="checkbox"/> Live	Notifications
<input type="checkbox"/>	prod_logs	http://elastics...	Yes	prod	0 Sources	<input type="checkbox"/> Inactive	Notifications

## Routes

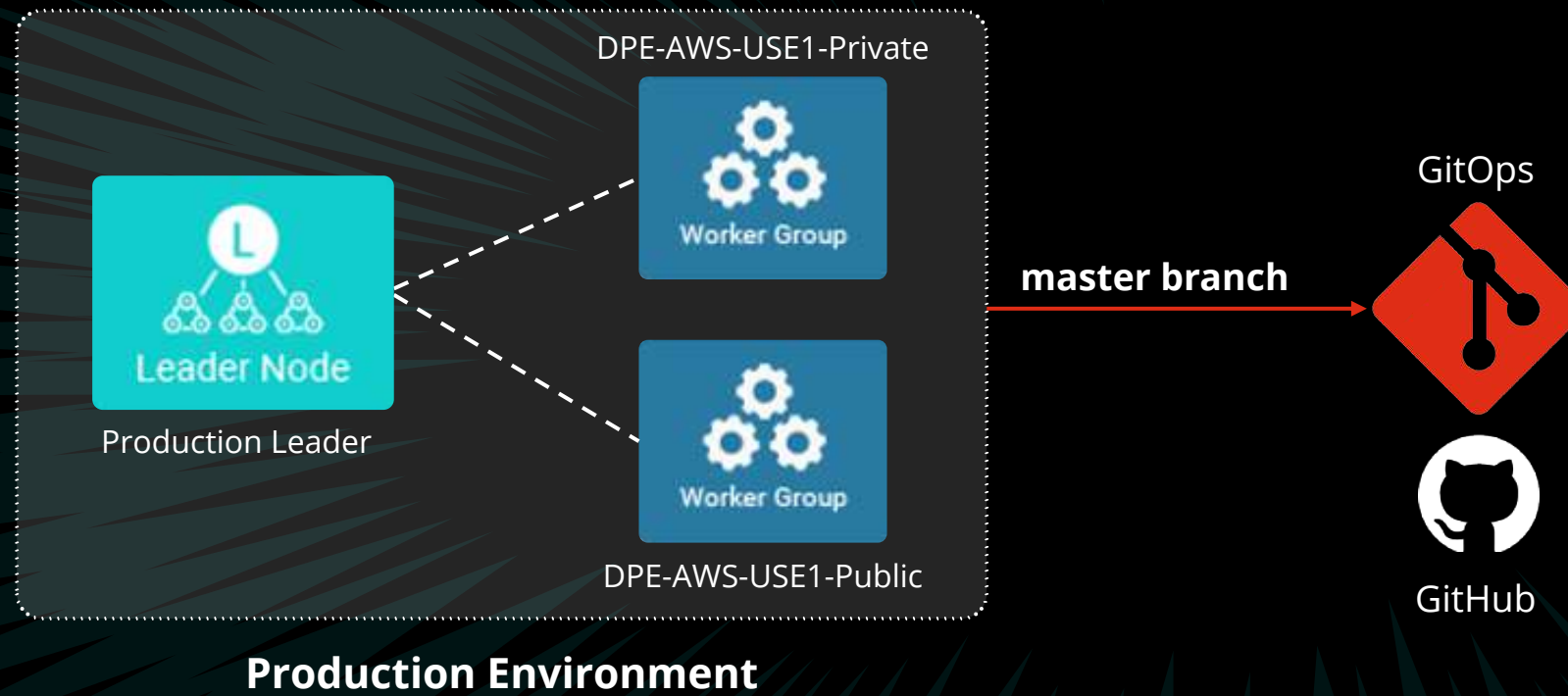
- Output Expression to understand bucket

The screenshot shows the 'Data Routes' configuration interface. At the top, there is a search bar and an 'Add Route' button. Below this is a table with columns for 'Route', 'Filter', 'Pipeline/Output', and 'Events (In)'. The 'apache\_logs' route is selected, showing a filter of 'true', a pipeline of 'apache\_logs', and 61.219% events. The configuration details for this route are shown below the table:

- Route Name\*: apache\_logs
- Filter: true
- Pipeline\*: apache\_logs
- Enable Expression: Yes (checked)
- Output Expression: `'${C.env.CRIBL_GIT_BRANCH}_logs'`
- Description: Enter a description
- Final: Yes (checked)

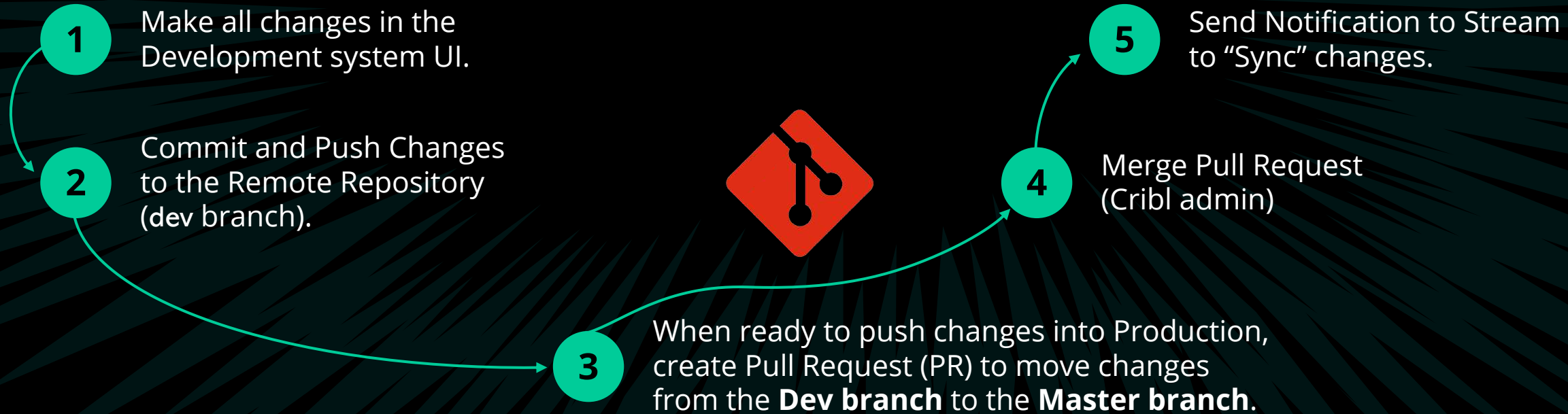
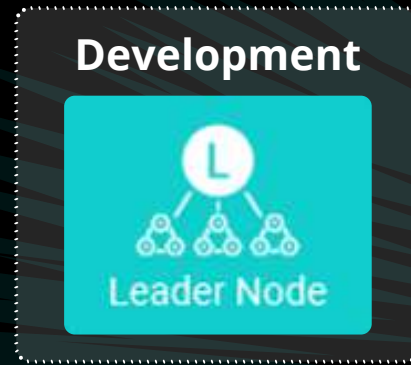


# CRIBL WITH GITOPS PRODUCT CAPABILITIES

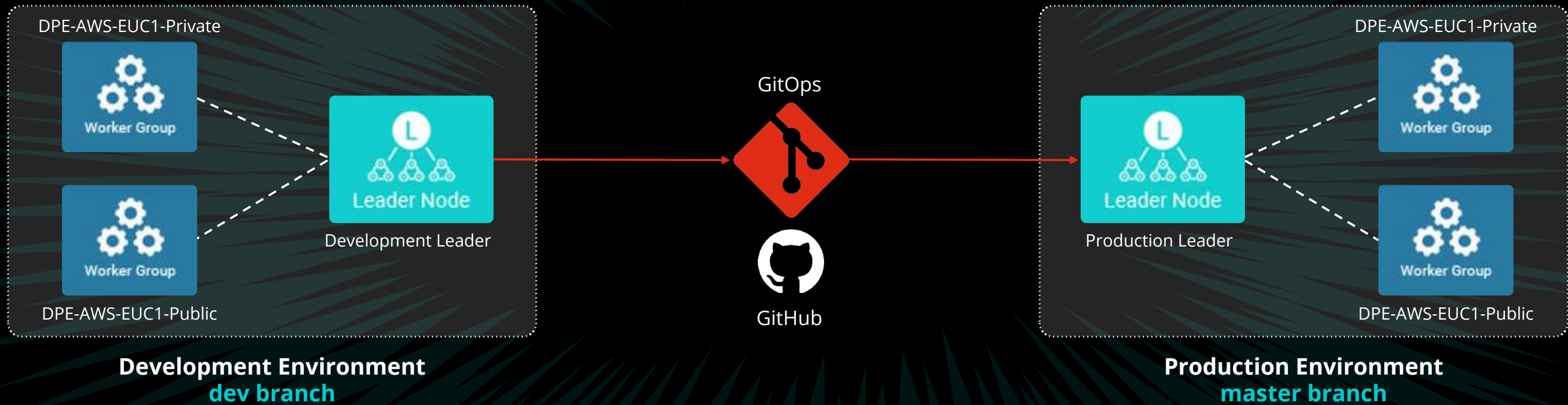




# GITOPS-FUTURE MODE OF OPERATION (FMO)

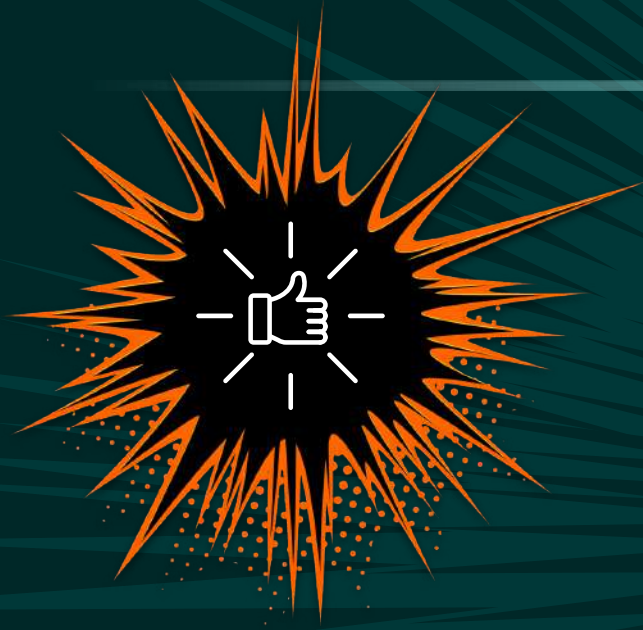


# GITOPS-FUTURE MODE OF OPERATION (FMO)





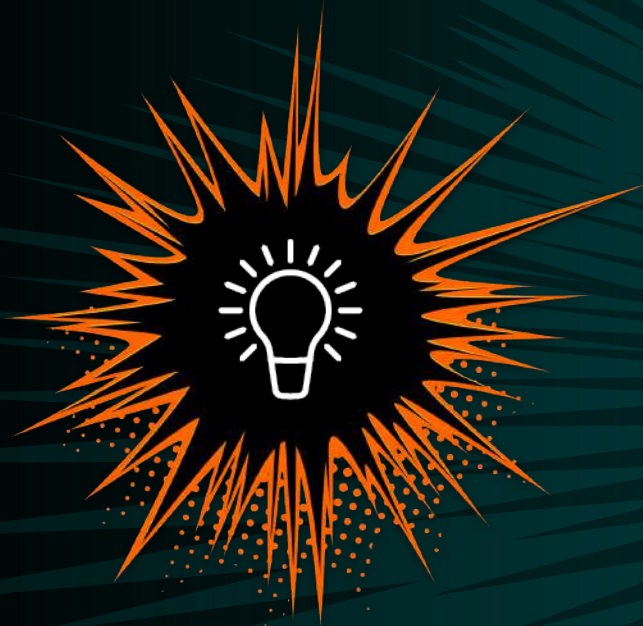
# BEST PRACTICES



## 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