How to use this deck

Name:

Lab Guide - Gitops with Event Driven Ansible

Purpose:

This deck is for teaching an Ansible Lab "Gitops with Event Driven Ansible" for Ansiblefest 2023

Last updated:

May 19th, 2023

What this deck is for?

Training, it goes hand-in-hand with self-paced exercises

What is this deck is NOT for?

Business level discussions

Google Slides source link (Red Hat internal):

https://docs.google.com/presentation/d/1wrJ90OEvkais6wcyinMq42uv1_VJJQlzrxHy8UgC220/edit?usp=sharing

Owner:

Ansible Business Unit, ansible-pmm-tmm@redhat.com
Colin McNaughton

Red Hat
Ansible Automation
Platform

Red Hat
Ansible Automation
Platform

Event-Driven Ansible for Gitops

Ansible Self-Guided Labs

Colin McNaughton
Principal TMM
@colincloin

Nuno Martins
Principal TMM

Event-driven Ansible for Gitops

01 What is Event Driven Ansible?

02 How does it work?

03 Lab 1 - Rulebooks: Getting started

04 Lab 2 - Gitops with Event Driven Ansible

05 Next steps

What is event-driven automation?

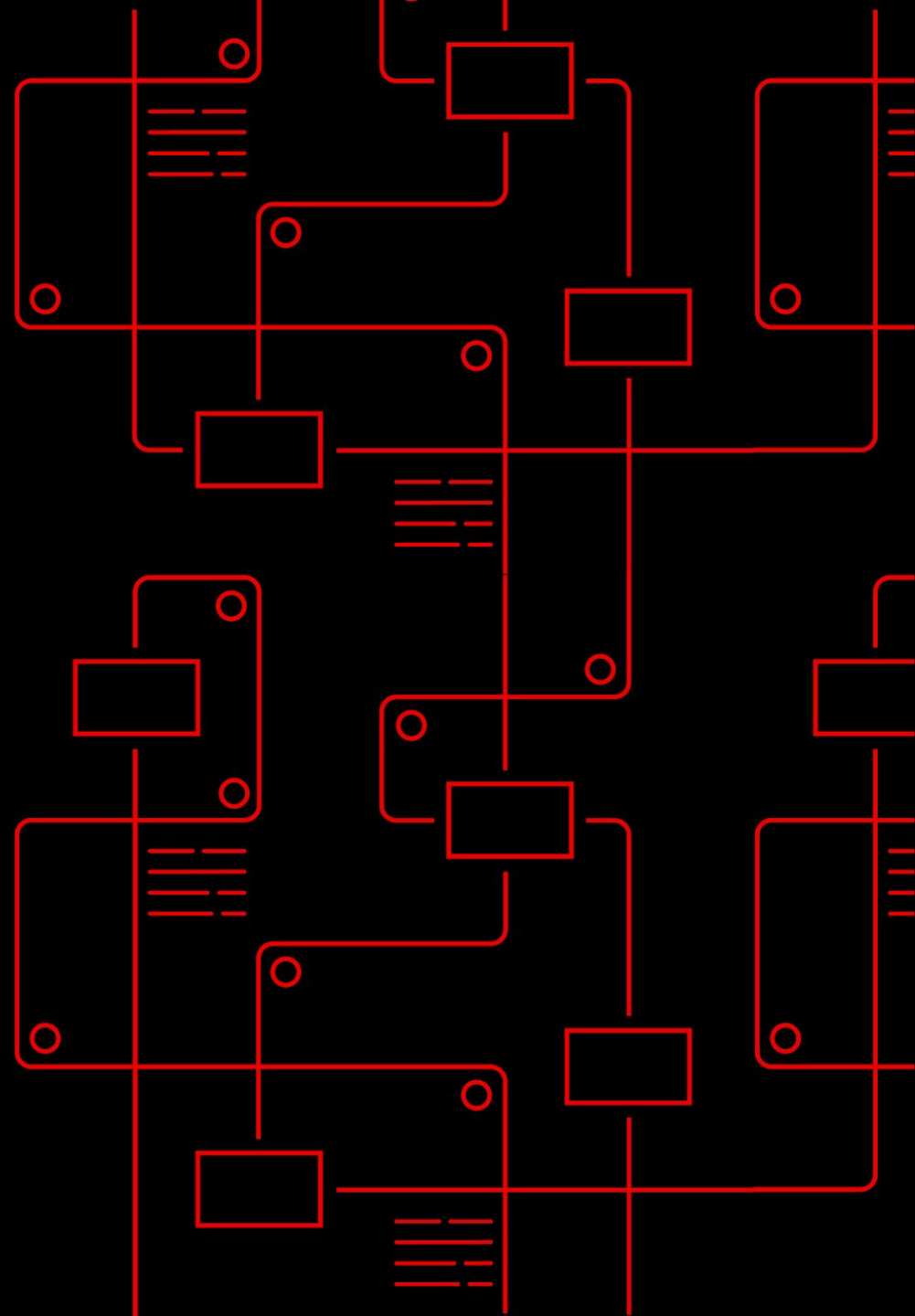
The ability to

connect intelligence, analytics and service requests

for an IT solution

to automated actions so that activities

can take place in a single motion.



A typical event-driven automation process

RECEIVE EVENT

- Work with third party sources of events
- Send important events to Event-Driven Ansible

DECIDE ON RESPONSE

- Known problem identified
- Automated resolution triggered

RESPOND AUTOMATICALLY

- Outage incident created
- Support team notified
- Remediation executed

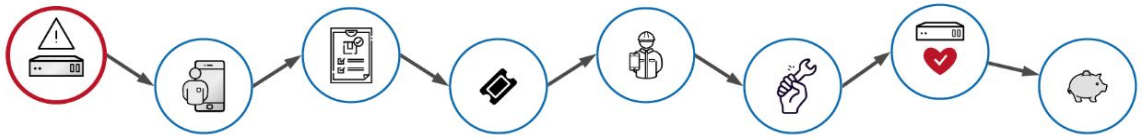
WORK ACROSS MULTI-VENDOR IT OPERATIONS

Work flexibly and well with multi-vendor monitoring and other solutions across the event driven architecture with appropriate approvals, controls and awareness

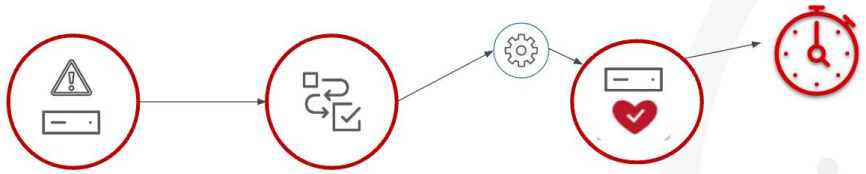
Red Hat

A brief history of IT Operations

The Old Way: Time, Toil and Churn



The new way: Event-Driven Automated Ops



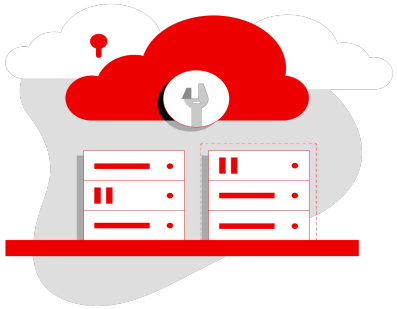
Outage resolution:
Follow a people-intensive multi-step manual process including opening tickets and multiple handoffs.

Event-Driven outage resolution:
Receive event, matching to rule, respond and act automatically

Security risk resolution:
Monitor to identify risk, notify and open a ticket, manually apply a patch or manually initiate automation job.

Event-Driven security risk resolution:
Receive risk event, match to rule, automatically apply patch to impacted inventory.

Suggested use cases for getting started

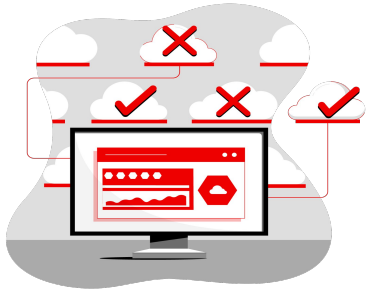


Service ticket enhancement

Automate fact gathering

Network administration

Edge device management

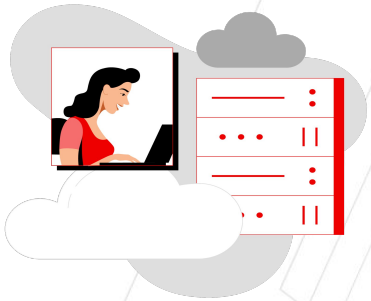


Remediation

Drift

Slow performance

Outages



User management

User authentication and access

Login issues

Group and role access

Event-Driven Ansible integrations and roadmap

CERTIFIED AND VALIDATED CONTENT
(Expected delivery Q2 and Q3 2023)

- Cisco NX-OS
- Cisco ThousandEyes
- CrowdStrike
- Cyberark
- Dynatrace*
- F5
- IBM Instana* and IBM Turbonomic*
- Palo Alto Networks
- Red Hat Insights
- Red Hat Openshift
- ServiceNow
- Zabbix
- AWS SQS
- Azure Service Bus
- GCP Pub/Sub
- Kafka (AMQ Streamz
- Prometheus/Alertmanager
- Webhooks
- watchdog (file system watcher)
- url_check (url status check)
- range (event generation plugin)
- file (loading facts from yaml)

*Collection includes both certified and validated content.

COMMUNITY CONTENT

- Arista

ROADMAP FOR INTEGRATIONS

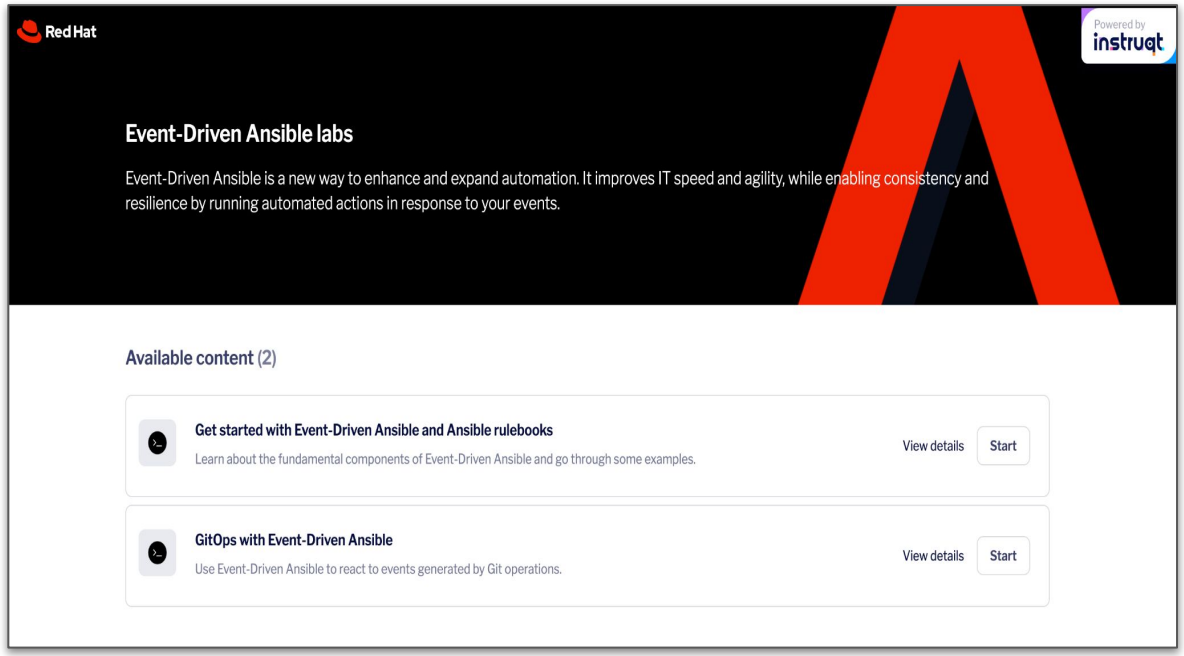
- Additional ITSM solutions
- Additional observability / monitoring tools

Blog: Event-Driven Ansible ecosystem partners

(as of May, 2023)

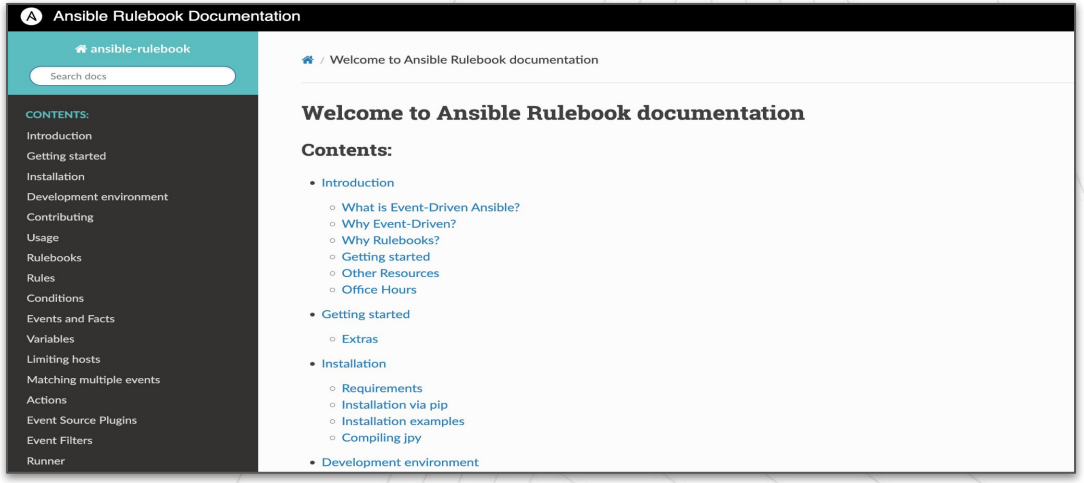
Red Hat

Three key technical learning resources



Interactive labs

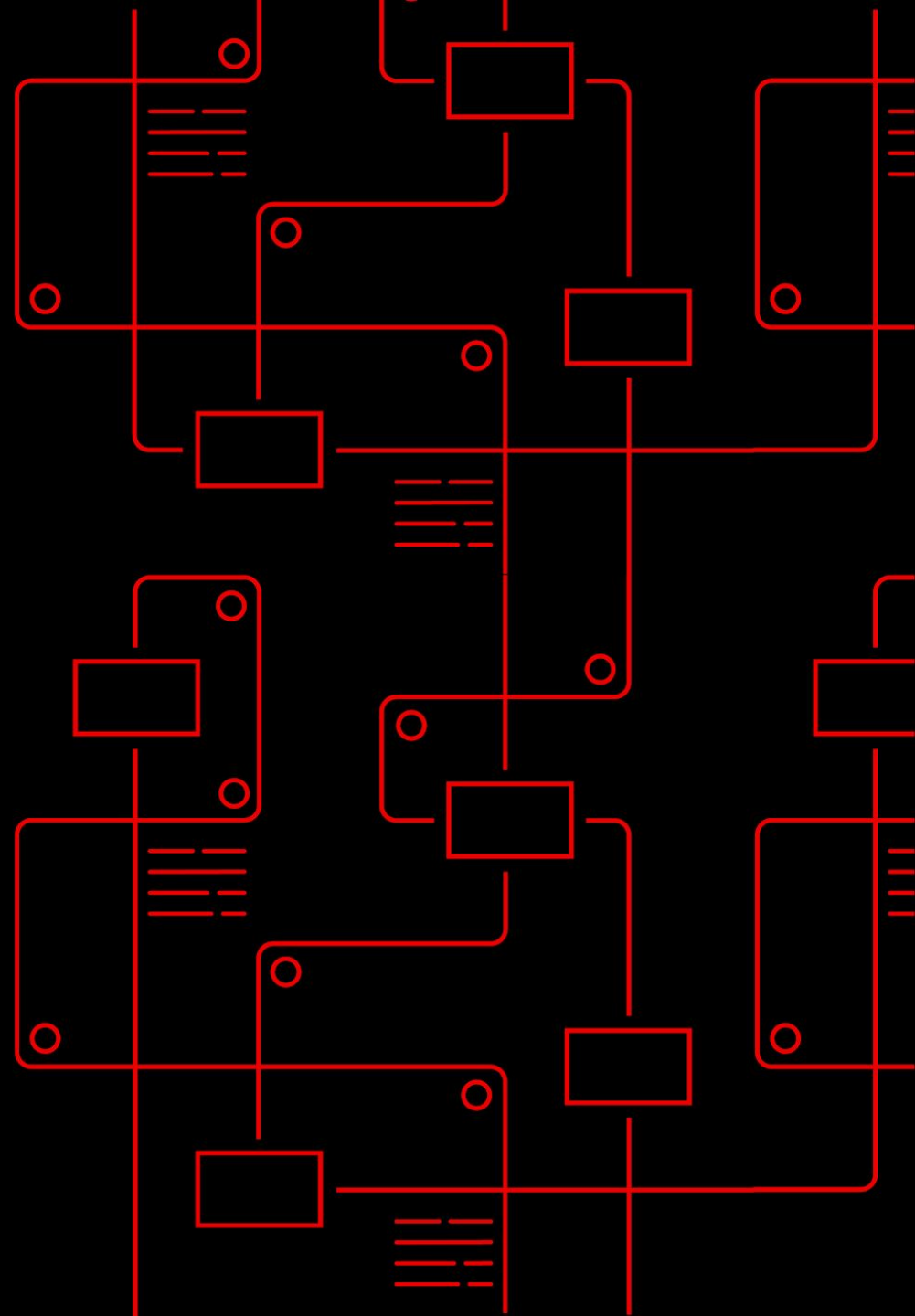
Technical blogs



Rulebook docs

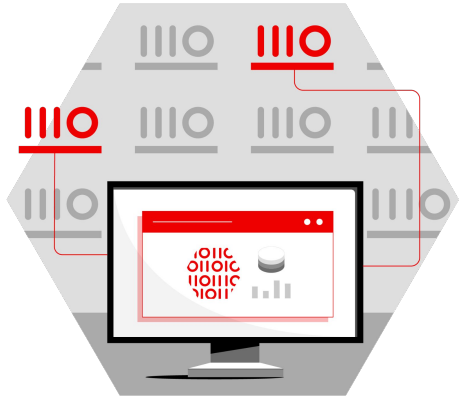
Red Hat
Ansible Automation
Platform

Ansible Rulebooks



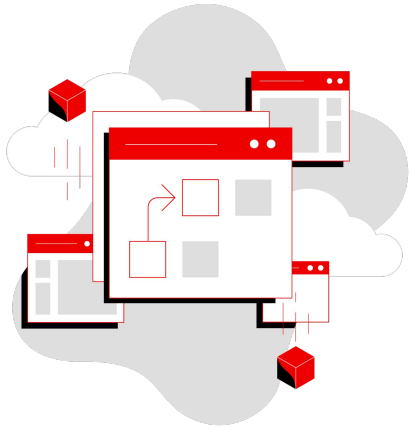
Key building blocks in Event-Driven Ansible

Simple, powerful, agentless



Sources

All the sources of event data you want to use



Rules

What you will create using Event-Driven Ansible®

Actions

When a condition or event is met, the Ansible Rulebook executes

Ansible Rulebooks contain the source of the event, as well as the instructions on what steps to perform when a certain condition is met–and it is all very flexible.

Ansible Rulebooks

Simple declarative decisions through rules

- **Events are processed by a rules engine**
  - Rules trigger based on conditions and actions can be carried out by the rules engine
  - Rules are organized into Ansible Rulebooks
  - Ansible rules can apply to events occurring on specific hosts or groups
- **Conditional management of actions to events**
  - Simple YAML structure for logical conditions
  - Events can trigger different types of actions:
    - Run Ansible Playbooks
    - Run Modules
    - Post new events to the event handler
- **YAML-like format familiarity**
  - Current Ansible users quickly learn and use Rulebook writing

```yaml
- name: Automatic Remediation of a web server
  hosts: all
  sources:
    - name: listen for alerts
      ansible.eda.alertmanager:
        host: 0.0.0.0
        port: 8000
  rules:
    - name: restart web server
      condition: event.alert.labels.job == "fastapi" and
event.alert.status == "firing"
      action:
        run_playbook:
            name: ansible.eda.start_app
```

Red Hat
Ansible Automation
Platform

Anatomy of an Ansible Rulebook

Smart automation from conditional rules

Receive | **Decide** | **Respond**

Event Source

```
...
source:
  - name: watchdog
    ansible.eda.watchdog:
      path: "{{src_path}}"
      recursive: true
      ignore_regexes: ['.*\.pytest.*', '.*__pycache__.*', '.*/.git.*']
rules:
  - name: Check for folder modification
    condition: event.type == "DirModifiedEvent"
    action:
      run_playbook:
        name: folder_permission_restore.yml
        post_events: true
  - name: Check for file Modification
    condition: event.type == "FileModifiedEvent"
    action:
      run_playbook:
        name: file_permission_restore.yml
        post_events: true
```

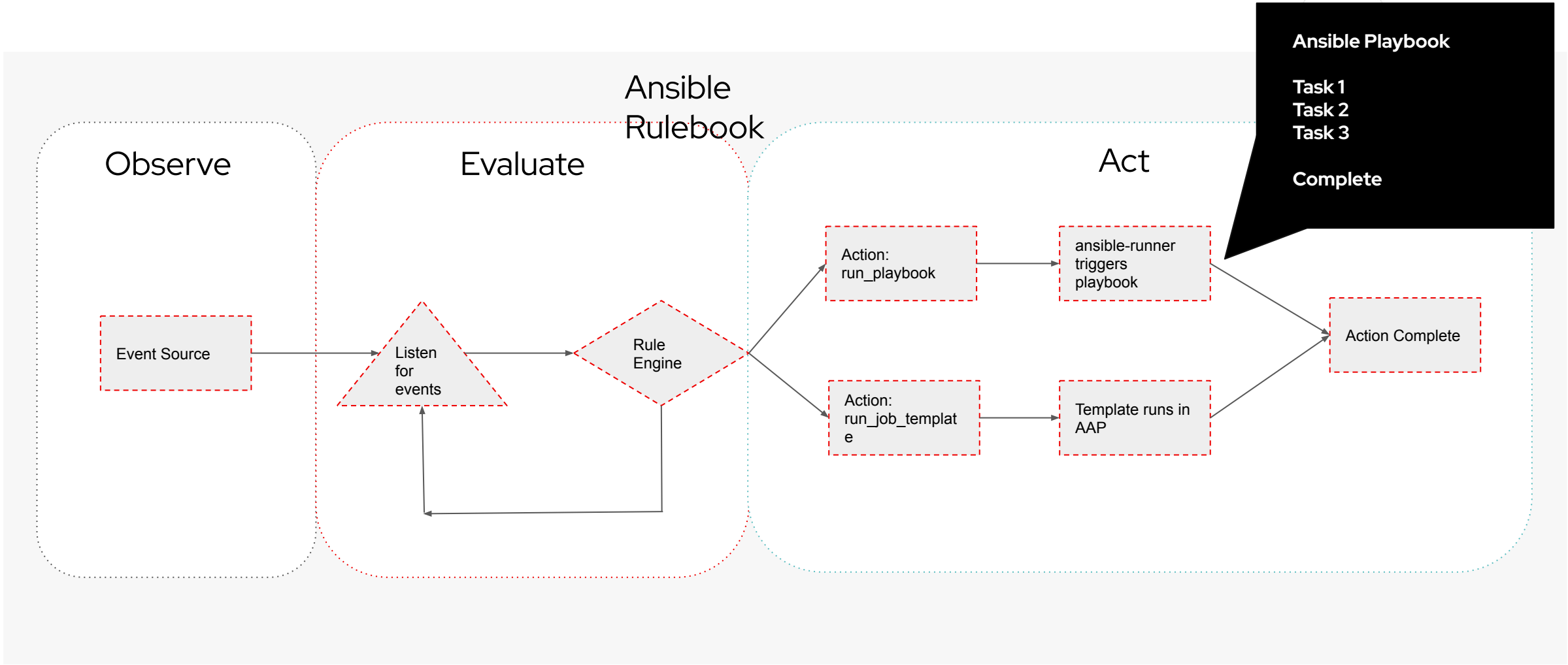
- Event sources are processed through conditional rules
- Actions are triggered once rule conditions are met

Automation

Red Hat

Event-Driven Ansible

Ansible Rulebooks can call playbooks to leverage and extend trusted playbooks



Red Hat
Ansible Automation Platform

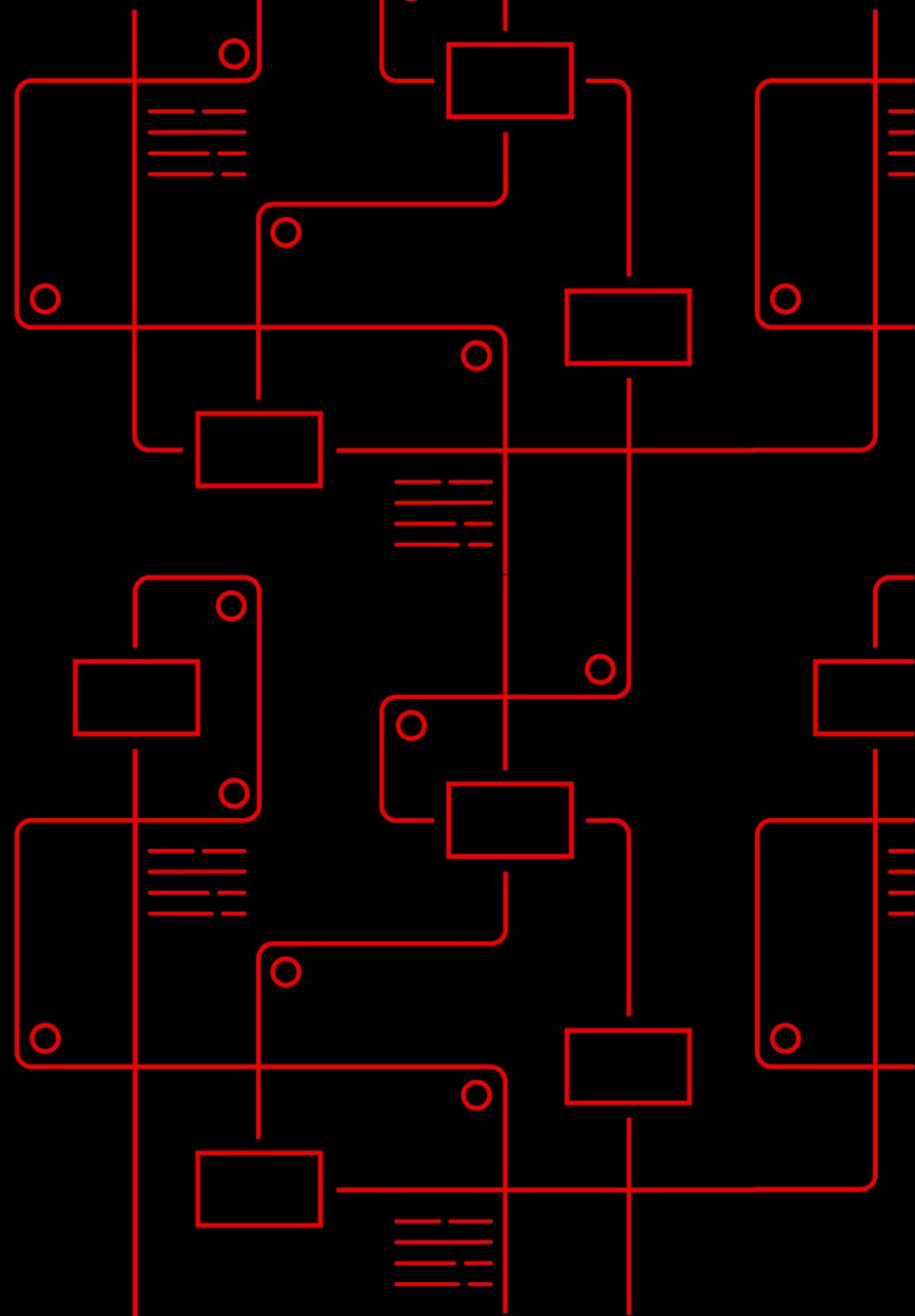
Lab Time

Lab 1 - Rulebooks: Getting started

15 Minutes

Red Hat
Ansible Automation
Platform

Event driven gitops



So what is **GitOps?**

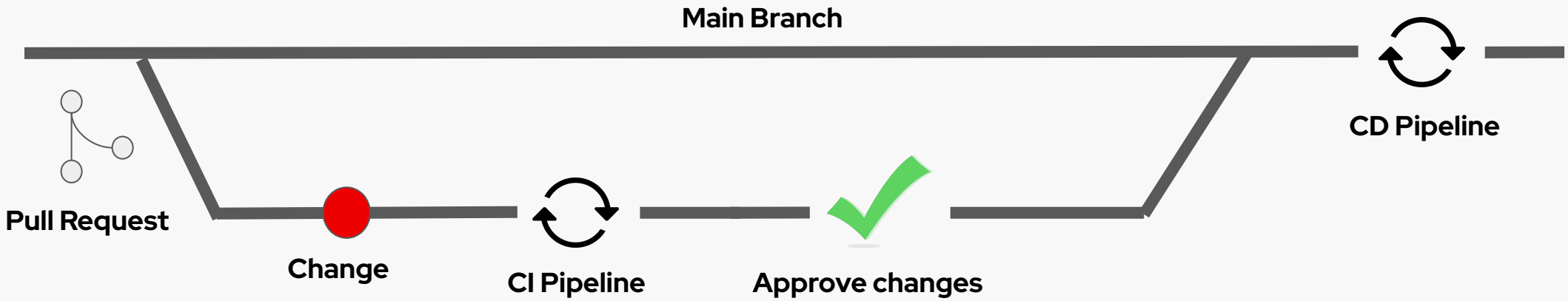
GitOps it is an operational framework that takes DevOps best practices for application development and applies them to infrastructure automation.

In other words?

Treat infrastructure as code as you would application code.

GitOps **workflow**

1. Create Pull Request
2. Run CI Pipeline
3. Approve changes
4. Run CD Pipeline

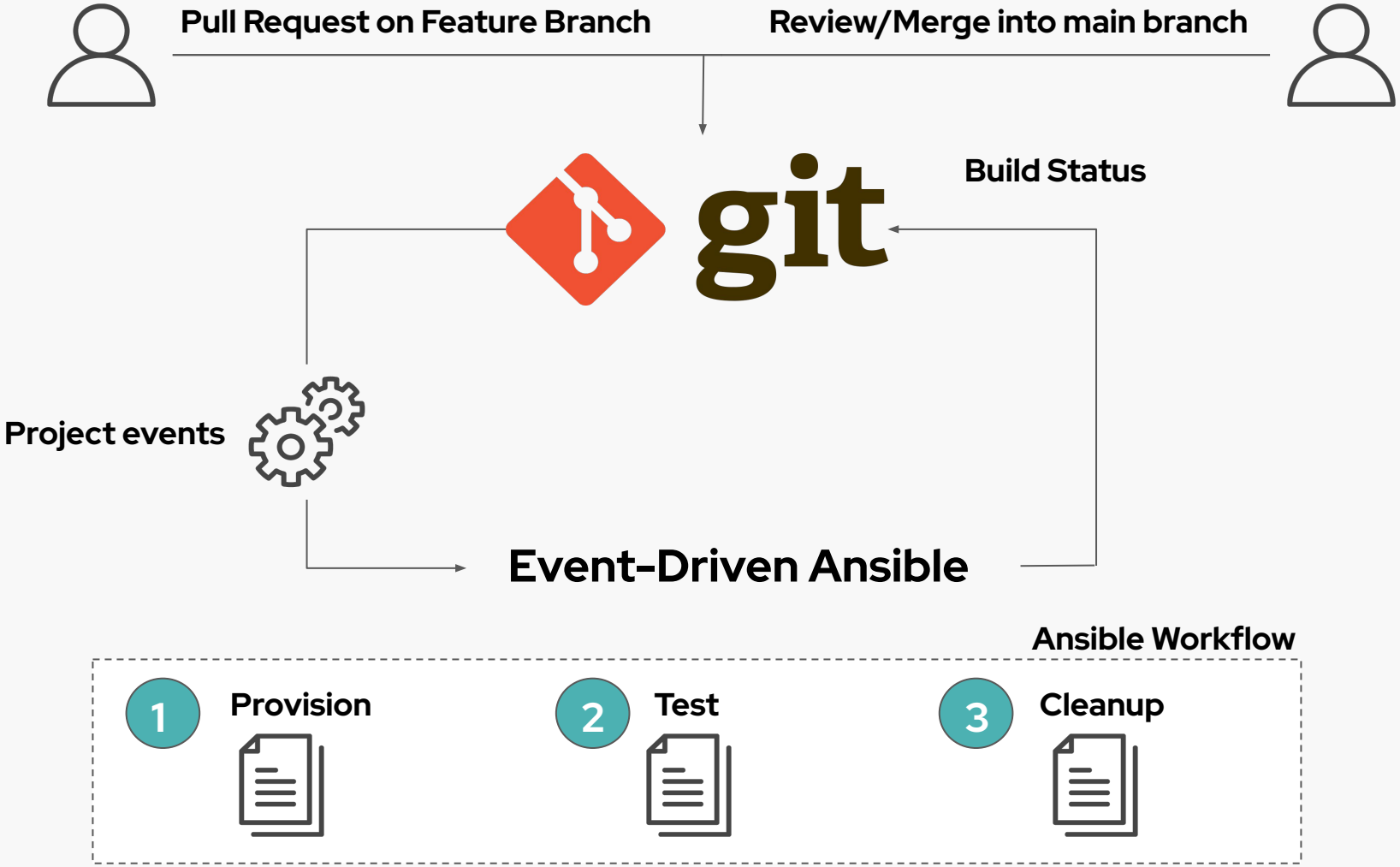


Red Hat
Ansible Automation
Platform

The benefits of **GitOps**

1. Increased productivity
2. Enhanced developer experience
3. Improved stability
4. Higher reliability
5. Consistency and standardization

Event Driven Ansible GitOps workflow

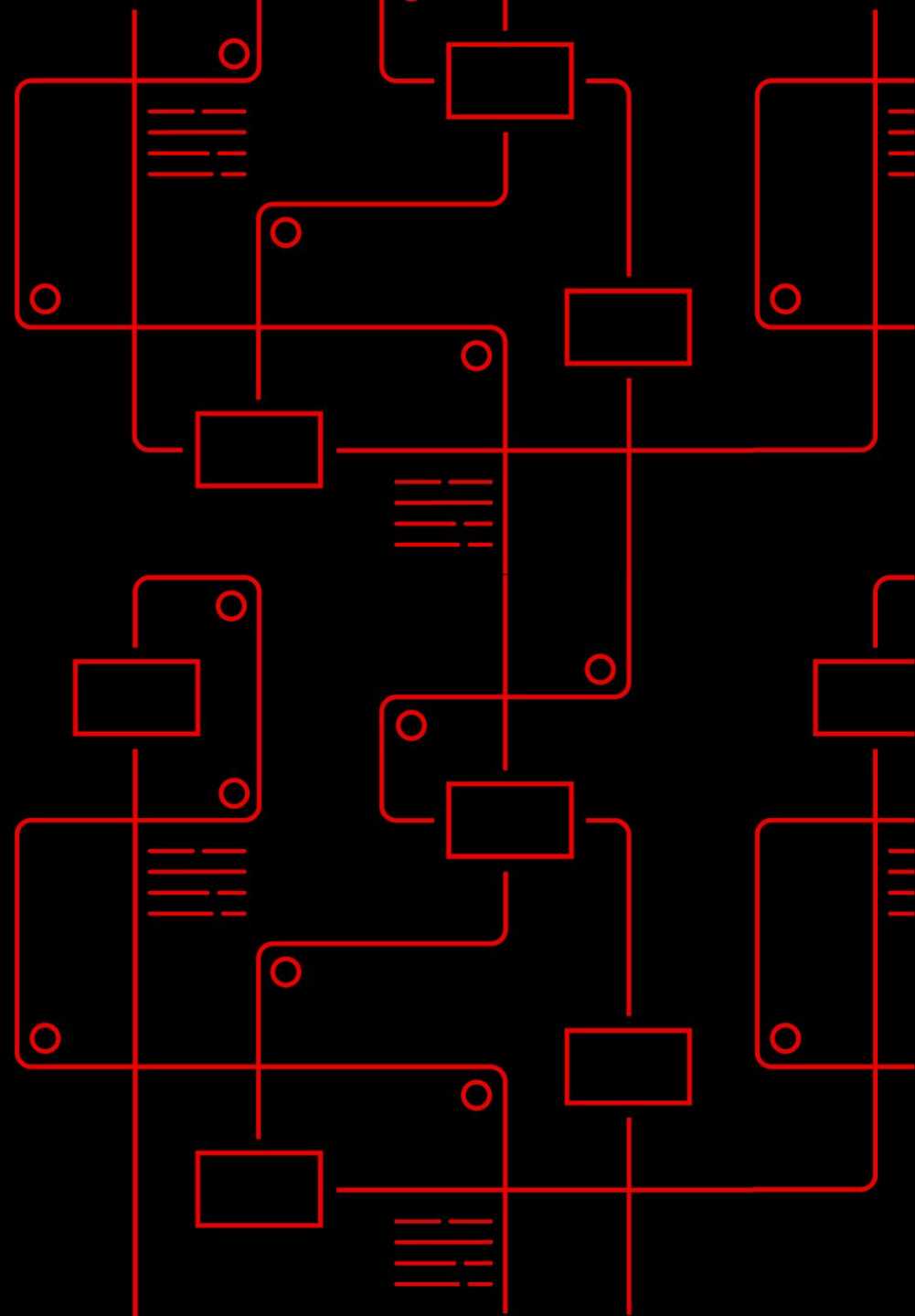


Lab Time

Lab 2 - Gitops with Event Driven Ansible

30 Minutes

Next steps



Learning resources

Continue your automation journey with Red Hat Ansible for public cloud automation

Ansible Automation Labs
red.ht/ansible_labs

E-book:
An IT executive's guide to automation
red.ht/automate_guide

Ansible Basics:
Automation Technical Overview
red.ht/automation_basics

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/c/AnsibleAutomation

facebook.com/redhatinc

twitter.com/ansible