DevSecOps with AWS Cloud

As we go forward for roles like **DevSecOps Engineer, SRE, Administrator** etc., we must work on Operating Systems like Linux and Windows.

Types of OS we have?

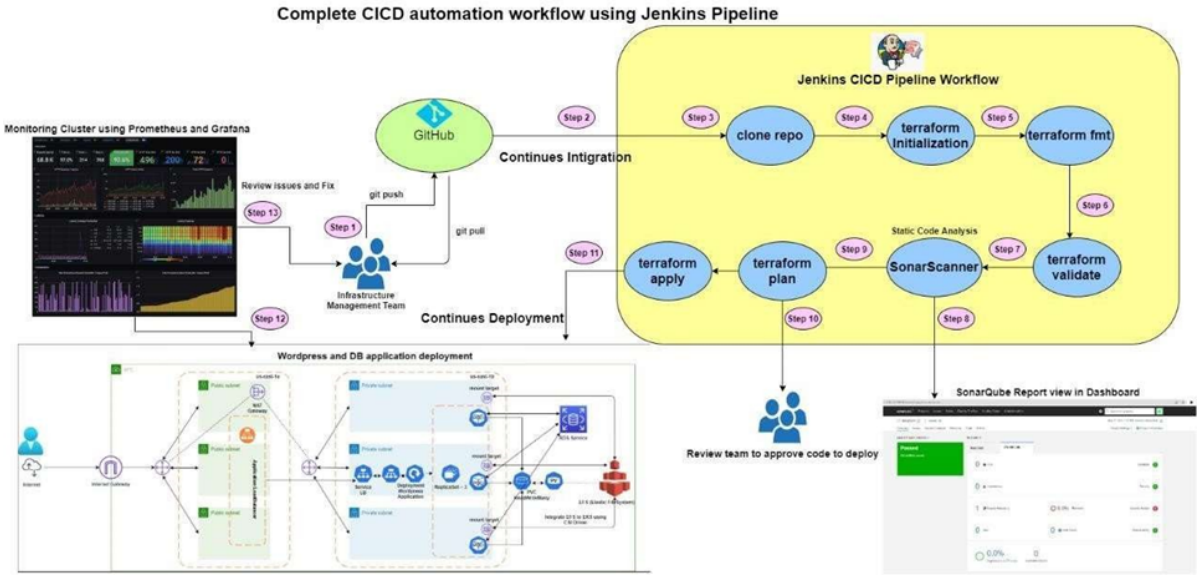
Single user Single task OS: In this OS system only one user can login to the system and run only one application on the server.

Single user Multitask OS: In this OS system only one user can login to system and run multiple applications like browser, games etc.,

Multiuser Multitask OS: This type of OS allows multiple users to login to the system and each user can perform various tasks at a time.

So, let's choose the Linux **Operating System** as per demand. Linux OS comes under Multiuser Multitasking Operating System.

In Linux, we have different flavors. We chose **Ubuntu** as it is easy to manage and understand the Linux fundamentals for Freshers and moreover. Not only that it was used in every Organization as a first choice to manage applications.



Linux OS:

1. Linux Architecture (Linux Flavors and Kernel)
2. Understanding core principle of Linux OS
3. Ubuntu 20.04 or 22.04 LTS version Installation as of today on Oracle VirtualBox [Ubuntu 20.04 Server] and [Oracle VirtualBox Download]
4. SSH and Password based authentication
5. Basic commands to handle Linux OS like cat, ls, date, free, top etc.,
6. Core fundamentals for Root Filesystem (/) like /root, /proc. /lib, /bin etc.,
7. Accessing Server and Managing networking (IP addresses and Classes etc.,)
8. Understanding basic commands as initial stage like ssh, ls, ip, cp, mv, mkdir, apt etc.,
9. Package management on Ubuntu
10. Installing packages on Ubuntu and understand the default files and folders to be managed Nginx/Apache, MySQL, WordPress applications
11. Linux file editors like nano, vi, vim
12. Linux File permissions and ownership management with chown and chmod commands
13. System and Network troubleshooting commands
14. Disk Management: partitions and LVM (Logical Volume Manager)

Shell Scripting:

1. What are commands and shell scripts?
2. Types of shells support in Linux OS
3. Difference between sh and bash
4. Permissions and execution
5. Variables and Arrays
6. Conditions and Loops
7. IO Redirection
8. Shell Functions
9. Exit codes
10. Important commands for scripting and daily operations like grep, awk, sed, find etc.,
11. Signals and numbers

Networking:

1. IP address types like IPv4 and IPV6
2. What is IPv4?
3. Classes
4. IP address
5. Public and Private IP addresses
6. Subnet
7. Broadcast
8. CIDR
9. Gateway IP address and NAT Gateway
10. Routers and Switches
11. DNS
12. Hostname
13. How to calculate IP address using simple formulas?
14. How to assign IP address and handle network in Linux OS Machines (VMs or Bare- Metal Servers)
15. Network troubleshooting tools like ping, netstat, nmap, traceroute etc.,
16. How to manage Virtual Network will be covered in AWS VPC Network

Ansible (Configuration Management Tool):

1. What is Configuration Management?
2. Opensource tools for Configuration Management
3. Why Ansible and Ansible architecture
4. Ansible setup and configuration
5. Add-hoc commands
6. Understanding hosts and ansible.cfg files

7. YAML Fundamentals
8. Variables and Facts
9. Groups_vars and host_vars etc.,
10. Modules
11. Roles
12. Playbooks
13. Tasks
14. Ansible Galaxy

Docker and Kubernetes:

1. What is Container and Images?
    a. Applications on Virtual Machines
    b. Applications on Containers
    c. What are container images?
2. Why must we run applications on Containers?
3. Docker and Use cases?
4. Docker Fundamentals
5. Docker public images from Docker Hub
6. Docker private images
7. Docker Containers
8. Docker Networking
    a. Host
    b. Bridge
    c. None
    d. Overlay
9. Docker Storage
    a. Volume mount
    b. Bind mount
    c. Tempfs mount

10. Docker Backup and Restore
    a. Data backup
    b. Images
    c. Containers
11. Docker Registry
    a. Local Registry
11. Custom Images build using Dockerfile
12. Scan tools like Trivy, Clair etc., to identify Vulnerabilities in Images
13. Docker Compose
14. Kubernetes Architecture
15. Kubernetes control plane and compute plane components
16. Kubernetes setup on local system using kubeadm
17. How to connect/reach k8s cluster using KUBECONFIG file
18. Kubernetes authentication and authorization
19. Kubernetes workloads
    a. Pods
    b. Replication Controller
    c. ReplicaSet
    d. Deployment
    e. Daemonset
    f. Statefulset
    g. Jobs and Cronjobs
20. Kubernetes Storage

    a. Volumes
    b. PV, PVC and StorageClass
    c. CSI
21. Kubernetes ConfigMap and Secrets
22. Services
    a. ClusterIP
    b. NodePort
    c. LoadBalancer
    d. ExternalIP and ExternalName
23. Ingress Controller
24. Network Policy
25. CIS benchmarking tools like kube-bench etc.,
26. Rest of the topics will be part of EKS Cluster on AWS

Jenkins CICD:

1. What is CICD?
2. Jenkins components
3. Installing and Configuring Jenkins on AWS EC2 or VirtualBox
4. Jenkins authentication and authorization
5. Plugins
6. Global system settings
7. Jenkins Jobs

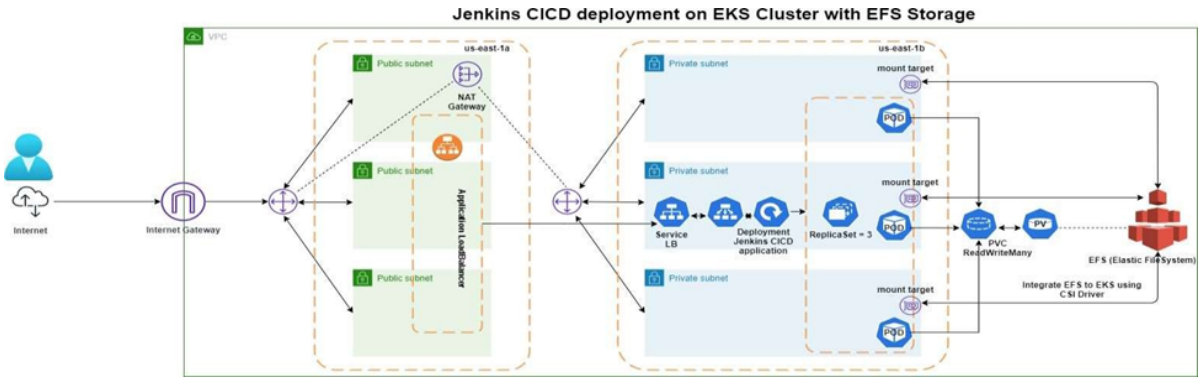
a. Free style Project

b. Multi-branch project

c. Folder

d. Pipeline Project

8. How to write a DSL (Domain Specific Language) pipeline for CICD automation?



SonarQube:

1) What is Static code analysis?
2) Tools available for static code analysis
3) SonarQube architecture and components
4) Sonar scanner for Terraform configuration analysis
5) Integrate SonarQube with Jenkins CICD for SCA
6) Analyzing report generate in Sonar Dashboard

AWS Administrative Services:

1. What is Cloud Computing?
2. What is IaaS, PaaS, and SaaS?
3. Why AWS Cloud?
4. AWS account creation and access
5. Secure AWS Count without root access
6. Understanding Compute, Monitoring, Authentication & Authorization services, and their dashboards
7. IAM (Identity and Access Management)
   a. What is Authentication and Authorization?

b. MFA and IAM administrative access

c. Users

d. Groups

e. Policies (Inline and JSON)

f. Roles

g. Account settings

h. STS (Security Token Service)

8. **EC2 Dashboard**

a. Differences between Bare-metal and Virtual Machines (Cloud and On-Premises)

b. Amazon Machine Image

c. Instance types (Flavors)

d. Security Group

e. Disk

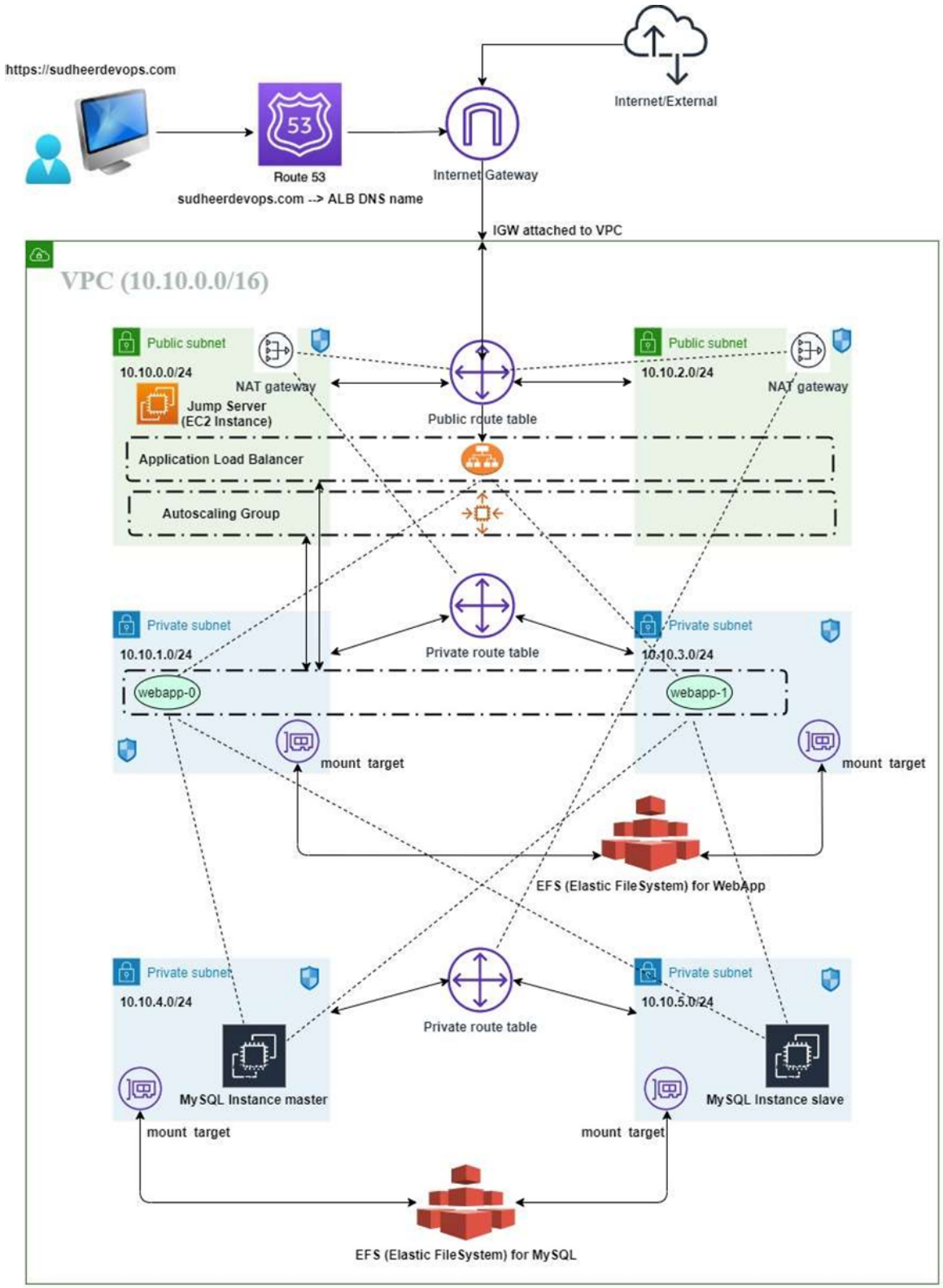
f. Key pairs

g. How to connect to EC2 Instances

h. Instance types like On-Demand, Reserved, Spot, Dedicated Instance and Dedicated host

i. Launch Template

j. Image creation from EC2 Instance



Webapplication Deployment over EC2 Instnaces using LoadBalancer and ASG

9. AWS VPC
    a. What is VPC?
    b. Network, Subnet, Route Table, Subnet Association
    c. Internet gateway and NAT gateway
    d. Elastic IP
    e. VPC Peering
    f. Transit Gateway
    g. ACL
    h. Egress Only Internet gateway
    i. Endpoints and Carrier gateway
    j. Endpoint Services
    k. Site-to-site VPN

10. AWS Storage services
    a. What is Object, Block and Filesystem Storage?
    b. S3 buckets
    c. EBS (Elastic Block Storage)
    d. EFS (Elastic Filesystem)
    e. AWS Storage Gateway
    f. AWS Transfer Family

11. Databases
    a. Understanding Relational and Non-Relational Databases
    b. Databases provided by AWS RDS

c. What is a Database Engine?

Microsoft SQL Server

e. How to connect databases from different remote locations?

f. Backup and restore functionalities

12. AWS LoadBalancer
    a. What is LoadBalancer?
    b. Difference between Layer 7 and Layer 4 load balancing?
    c. Types of LoadBalancer support in AWS

       CLB (Classic Load Balancer)

       ALB (Application Load Balancer)

       NLB (Network Load Balancer)

       GLB (Gateway Load Balancer)

    d. Target Groups
13. AWS Auto Scaling
    a. What is autoscaling?
    b. How does it help to spin multiple EC2 instances horizontally?
    c. Creating Launch Configuration
    d. How to create and manage Auto Scaling groups?
    e. Notifications
14. AWS CloudWatch
    a. What is CloudWatch?
    b. Alarms
    c. Logs
    d. Events

e. Metrics

f. Insights

g. Application Monitoring

15 AWS CloudTrail for auditing AWS account

16. AWS CloudFormation Templates

17. Container and Orchestration services

a. ECS (Elastic Container Service) and Fargate
b. ECR (Elastic Container Registry)

c. EKS (Elastic Kubernetes Service) and Fargate

Accessing EKS Cluster

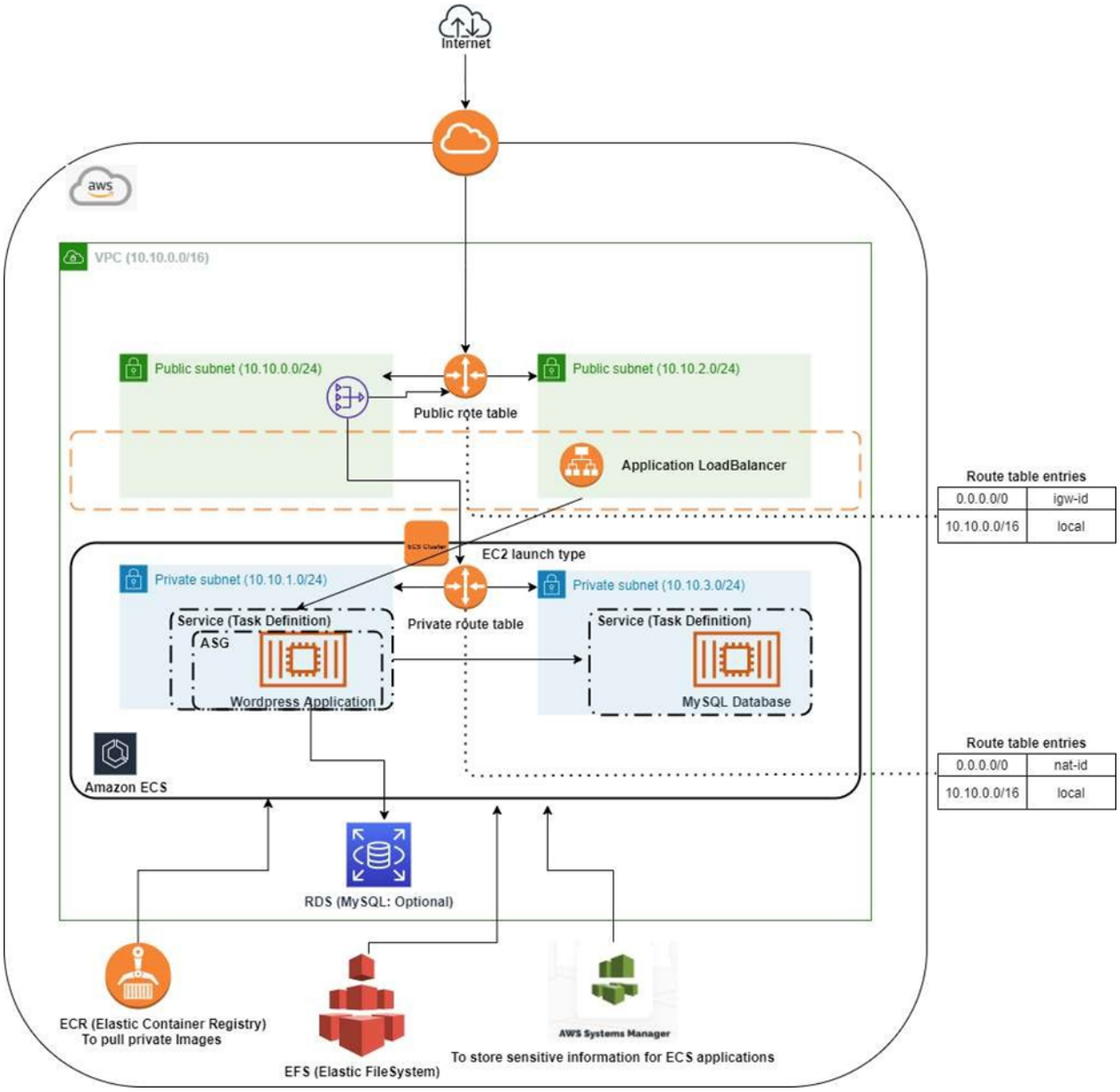
Private and Public EKS Cluster

VPC network

IAM roles and policies for EKS

Node Group

External DNS for AWS Route 53 for EKS Ingress hosts



18. AWS Route 53

    a. What is DNS?

    b. What are DNS domain zones?

    c. DNS troubleshooting tools

    d. Private and Public zones

    e. Internal and External Domains in AWS Route 53

19. AWS Notification services
    a. Simple Email Service
    b. Simple Notification Services
    c. Simple Queue Service
20. AWS Certificate Manager
21. AWS System Manager
22. AWS Backup
23. AWS ElastiCache

Git (Distributed Version Control System):

1) What is Version control system?
2) Difference between CVCS and DVCS?
3) Why Git?
4) Git workflow
5) Git commands (add, init, push, pull, commit, etc.,)
6) Git logs
7) Git repositories like GitHub, AWS CodeCommit
8) Branching strategies
9) Tagging code
10) Reset Vs Rebase
11) How to fix merge conflicts in git?
12) Integrate CI with Jenkins and GitHub

Terraform (Infrastructure as Code):

Ø What is Infrastructure as a Code?

Ø Opensource tools for IaC
Ø Why only Terraform?
Ø Terraform Setup and Configuration to communicate AWS Cloud provider
Ø Terraform workflow

Ø Terraform configuration language

- Ø Terraform top-level blocks
- Ø Terraform resources
- Ø Terraform variables
- Ø Terraform functions
- Ø Terraform values
- Ø Terraform datasources
- Ø Terraform backends
- Ø Terraform workspaces
- Ø Terraform modules public and custom
- Ø Terraform expressions
- Ø Terraform disaster recovery

Security tools for DevSecOps

We will be learning Security tools that need to run check on different stages like Infrastructure, Software, Application, etc., checks and automate the entire process using CICD

TIVY	Docker Security	Kube Bench	Kube Linter

1) Trivy for Image vulnerability scan as part Docker Image build
2) Build CICD workflow to build, scan, and push images to ECR
3) Implement CIS benchmark check on Docker Engine machine using Docker Security
4) Understanding the checks its status code which to be ignore and one which must be considered to fix
5) Integrating CICD to workflow to run check on Kubernetes cluster using Kube-bench tool
6) KubeLinter tool helps to analyze manifests files (YAML) and Helm charts as well

End-to-End Live Project deployment using DevSecOps automation tools