Stage : Cluster Security Before Deployment:

Objective of the stage :
Ensure that the Kubernetes cluster is secure and ready for application deployment by performing thorough security checks.

Cluster Security Audit:
Tools : Kube-Hunter
penetration testing tool that simulates attacks on a Kubernetes cluster to identify vulnerabilities

Security Policy Analysis
Tools : Open Policy Agent (OPA)
Verify that Kubernetes security policies, such as Network Policies, Pod Security Policies, and Role-Based Access Control (RBAC), are correctly configured and enforced.

Secret Management and Pod Configuration
Tools : HashiCorp Vault
HashiCorp Vault is a tool that allows you to manage your secrets securely. By secrets, we mean sensitive information such as digital certificates, database identifiers, passwords and API encryption keys. HashiCorp Vault allows you to store these secrets, then authenticate, validate and authorize access to clients and users

Checking the Cluster Configuration
Tools : kube-linter
Using kube-linter to parse Kubernetes configuration files

Threat Detection and Response

Tools : Falco

Deploy Falco for real-time intrusion detection and abnormal behavior monitoring in the Kubernetes cluster.