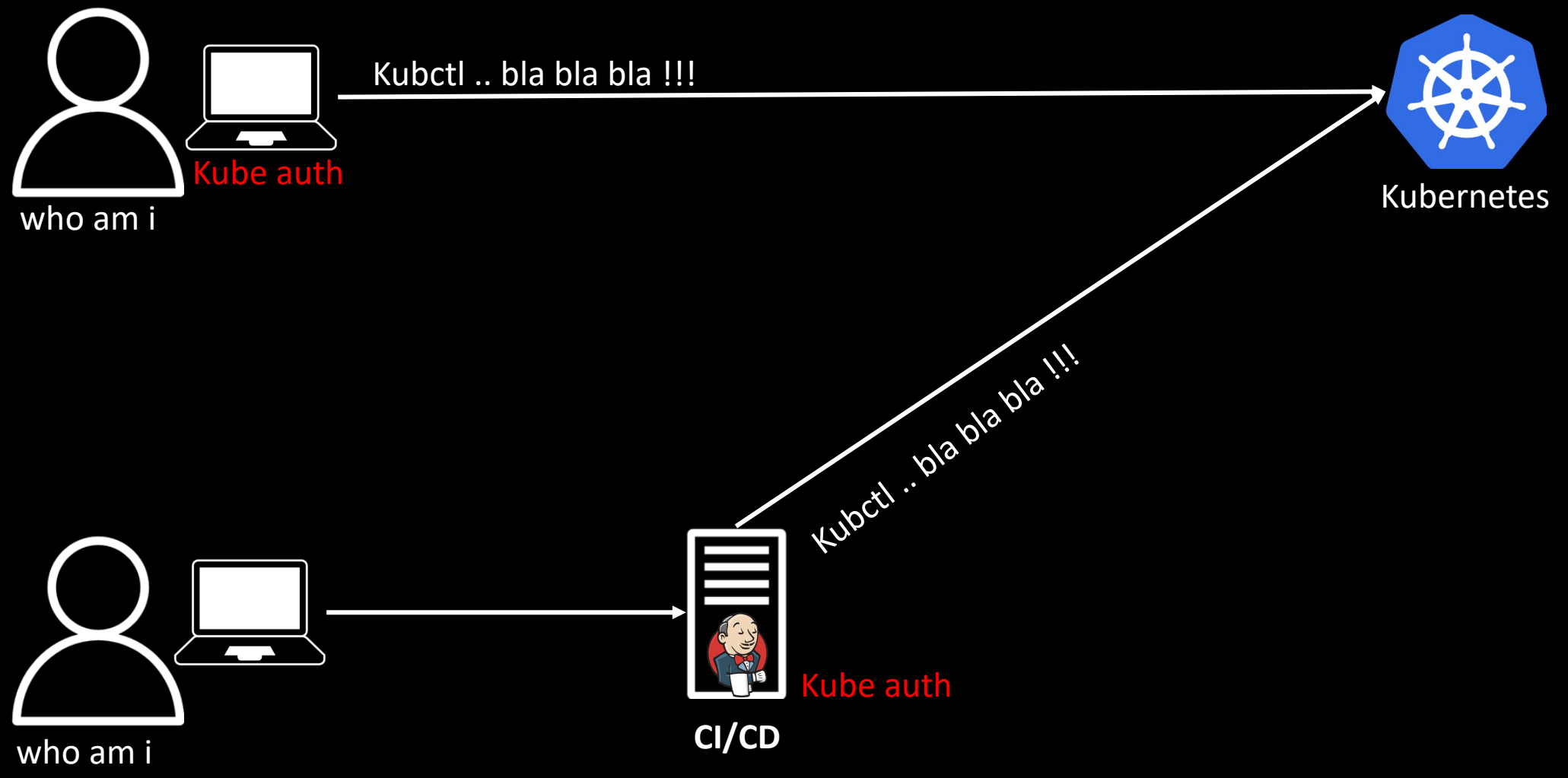
Zero-Trust and Secret Management for Applications

nimble
by krungsri

What's the problem definition?

nimble by krungsri

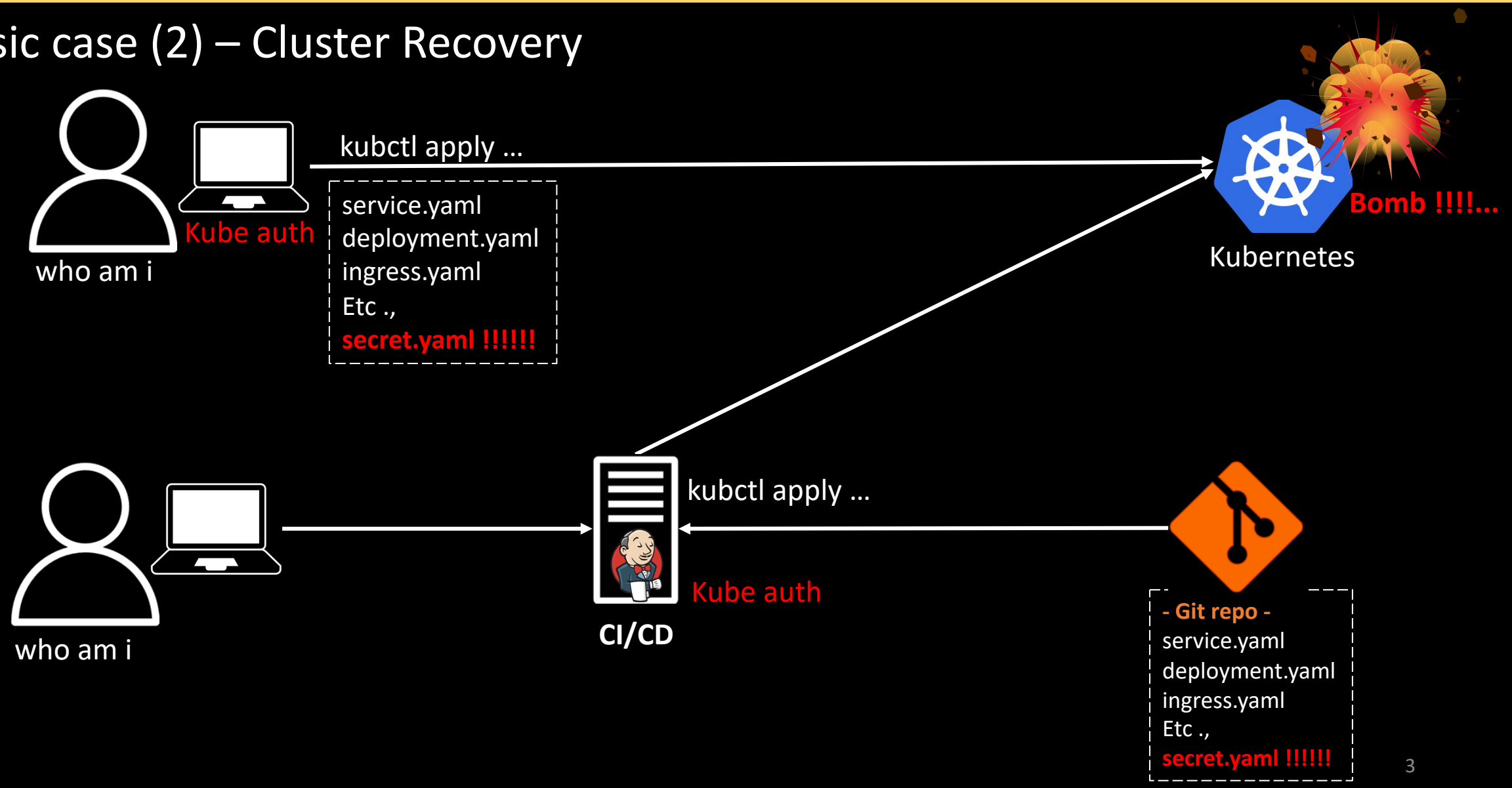
Basic case (1) – Kube Control



What's the problem definition?

nimble by krungsri

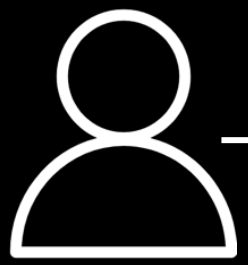
Basic case (2) – Cluster Recovery



What's the problem definition?

nimble by krungsri

Basic case (3) – Apply Kube Secret



who am i

Secret.yaml

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: mysecret
type: Opaque
data:
  USERNAME : YWRtaW4= #admin
  PASSWORD : UEBzc3cwcmQ= #P@ssw0rd
```

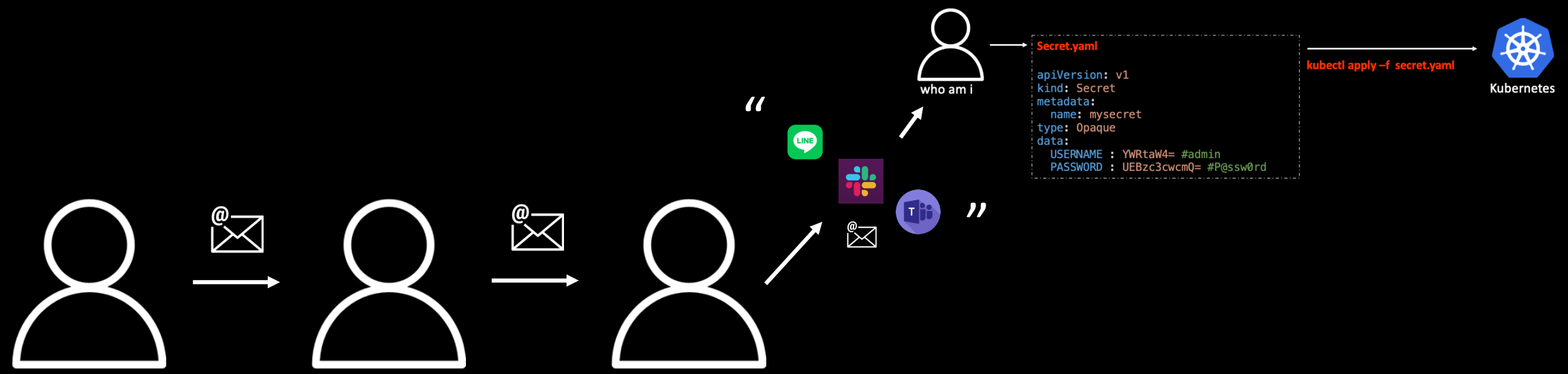
kubectl apply –f secret.yaml

Kubernetes

What’s the problem definition?

nimble by krungsri

Basic case (4) – Send password (**Assume)



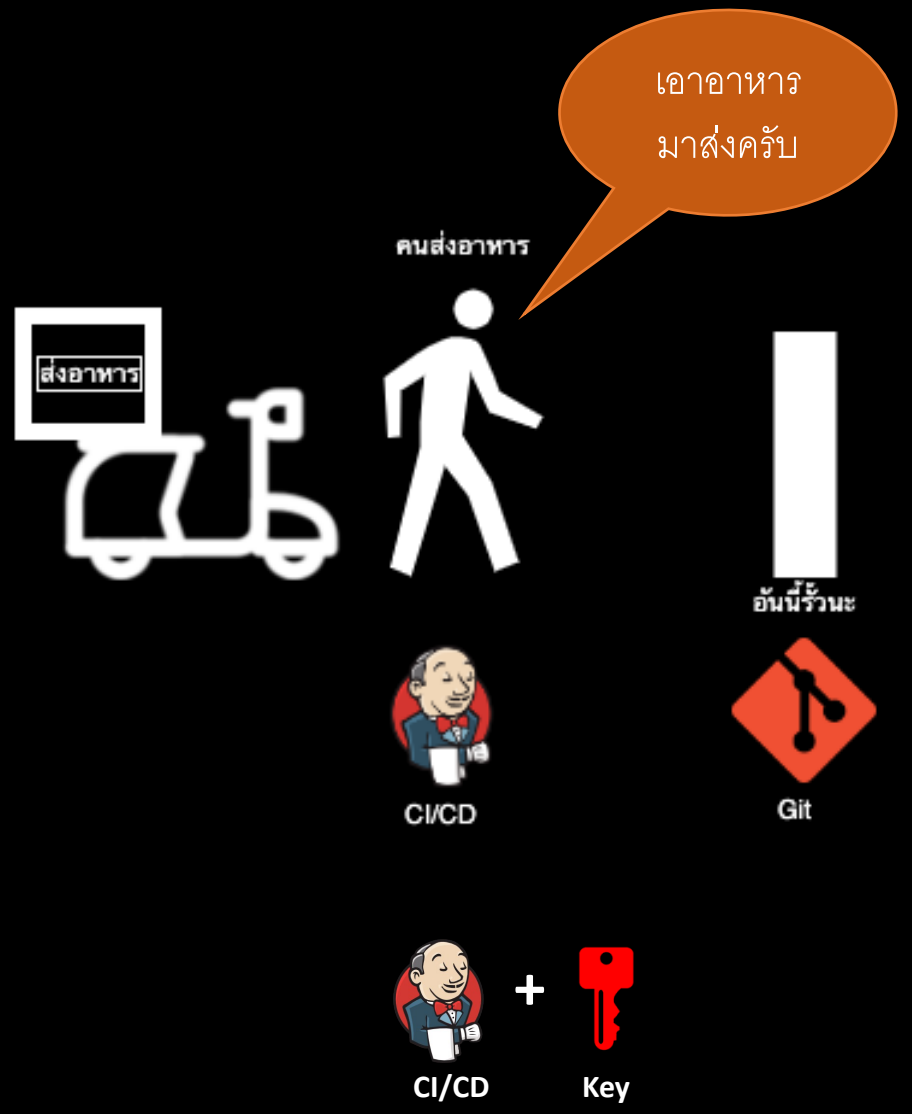
PPT Framework

nimble by krungsri

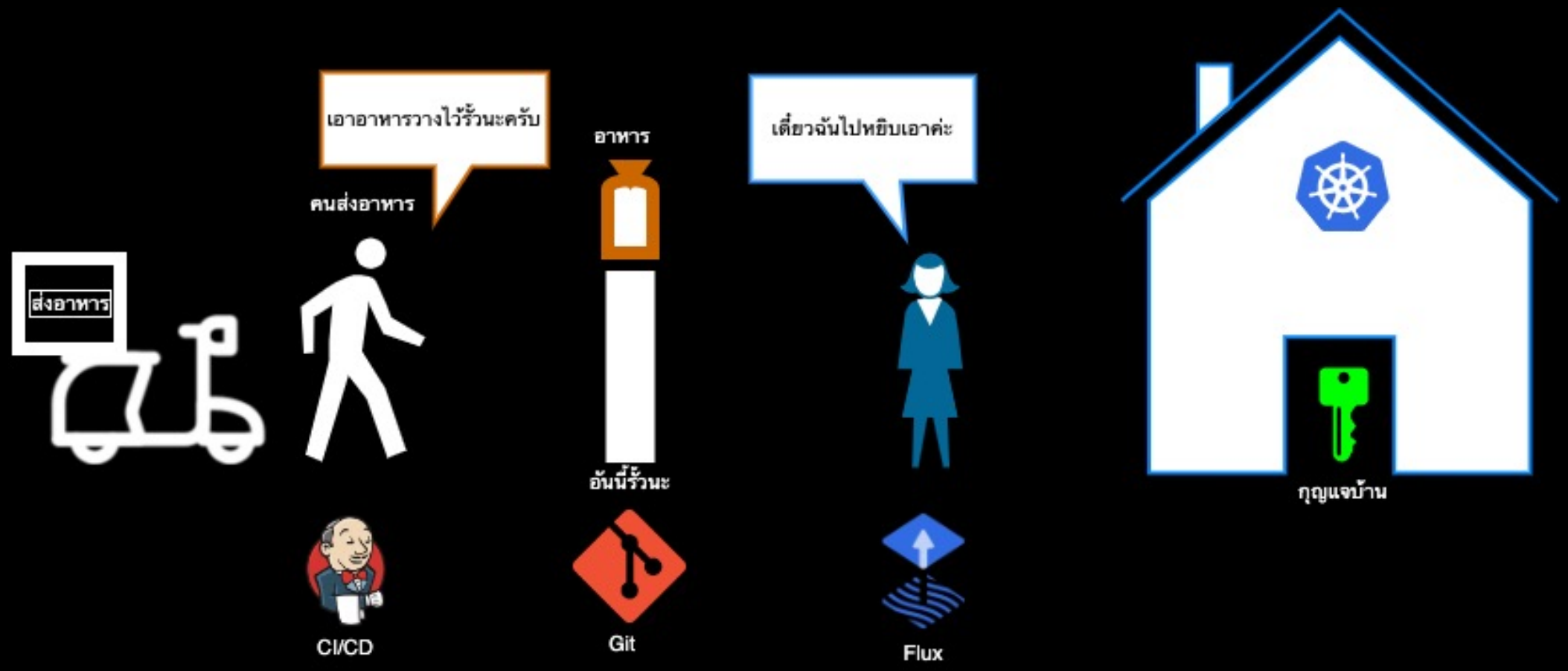
People	Process	Technology
• " I am Nimble " • Administrator • Production support • etc.,	• Solution Architech Review • Change Management • Approval process • etc.,	• Flux – GitOps (Flux has been promoted to Graduated status in the CNCF) • Amazon Web Services - Infrastructure • Kubernetes - Container Orchestration. • KMS – Key management • SOPS , AWS Secret – Secret management.

Flux Kubernetes EKS KMS Secret Manager

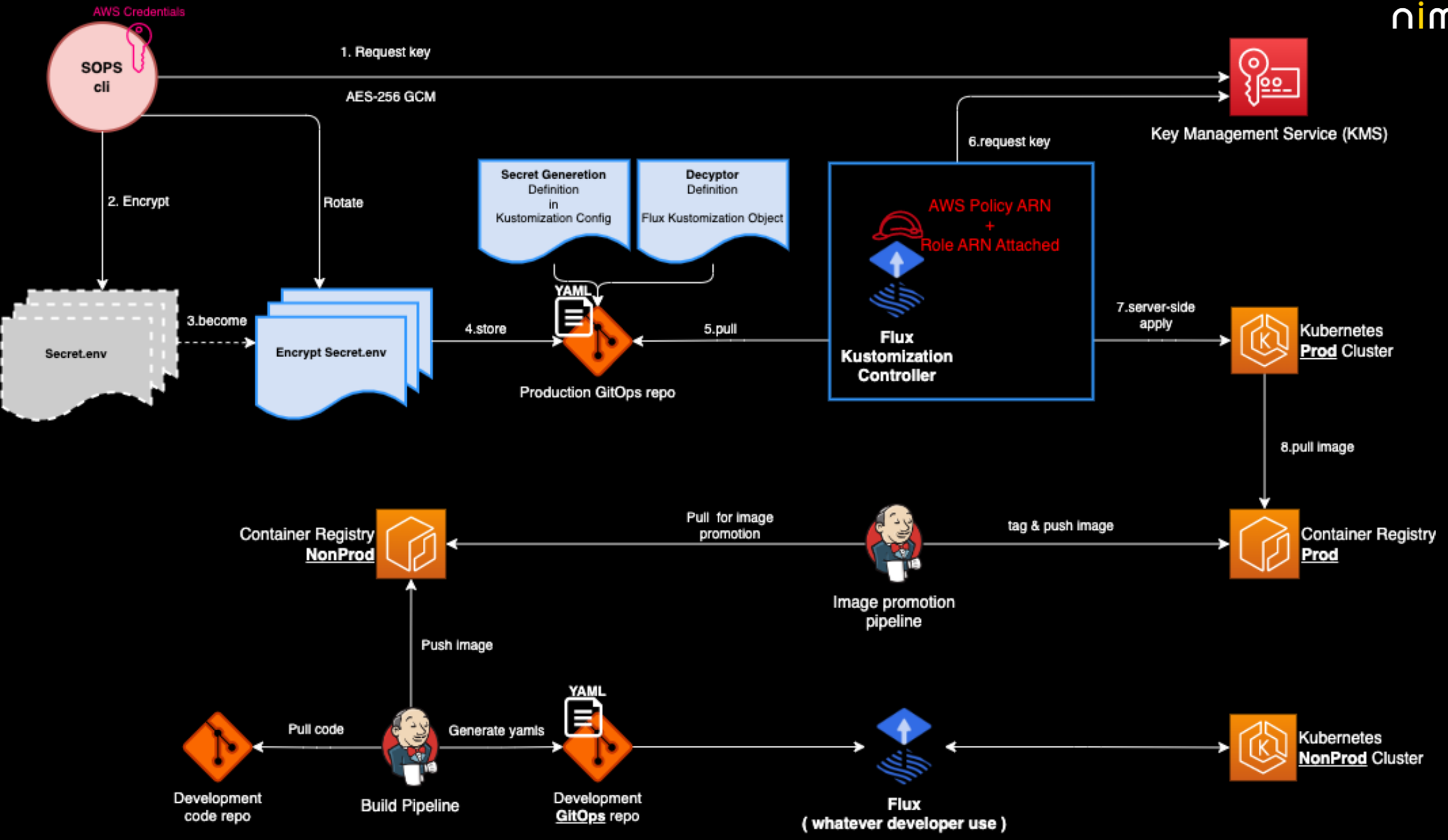
Zero Trust Concept



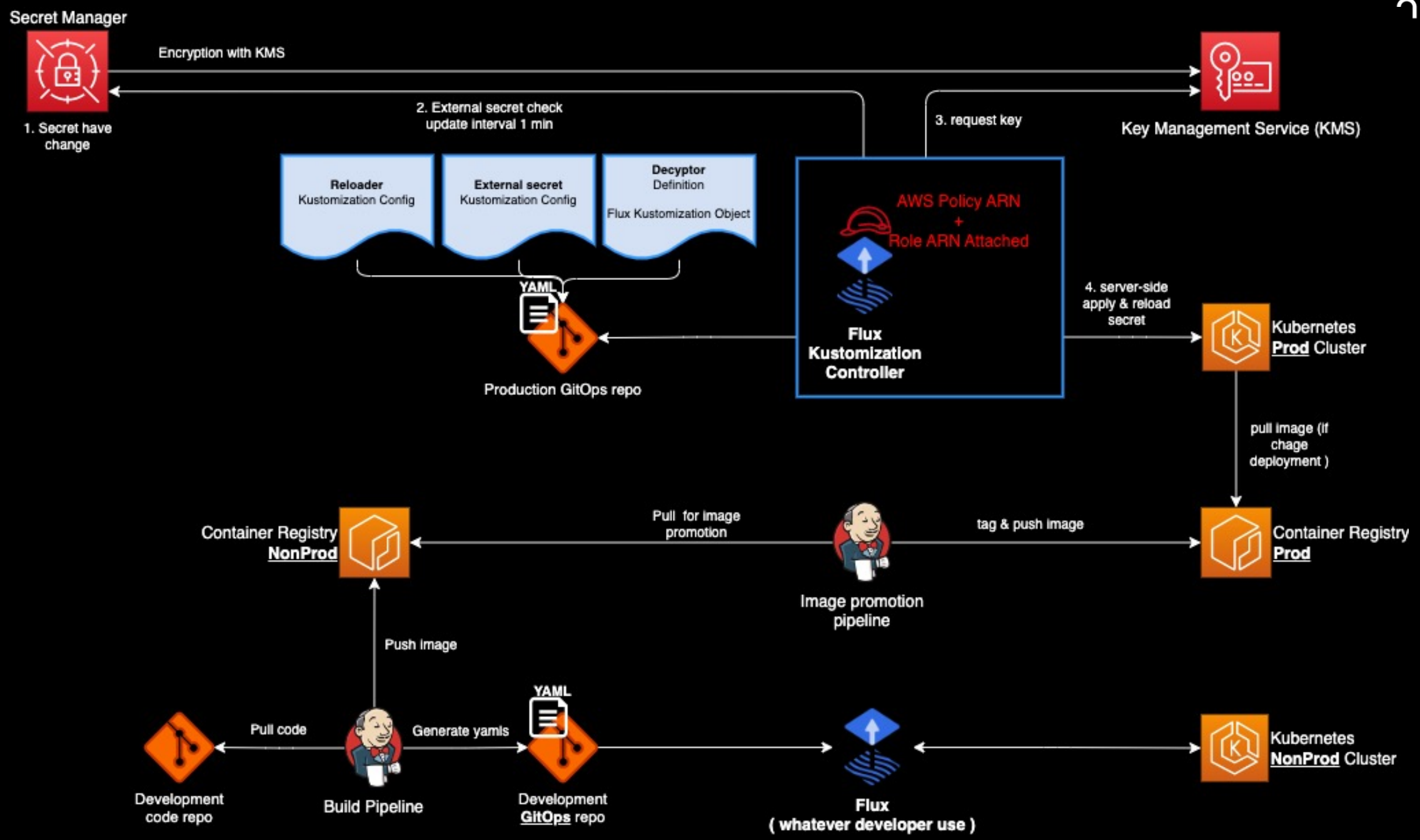
Zero Trust Concept



Solution (1) - Flux with SOPS CLI – ** Recovery **



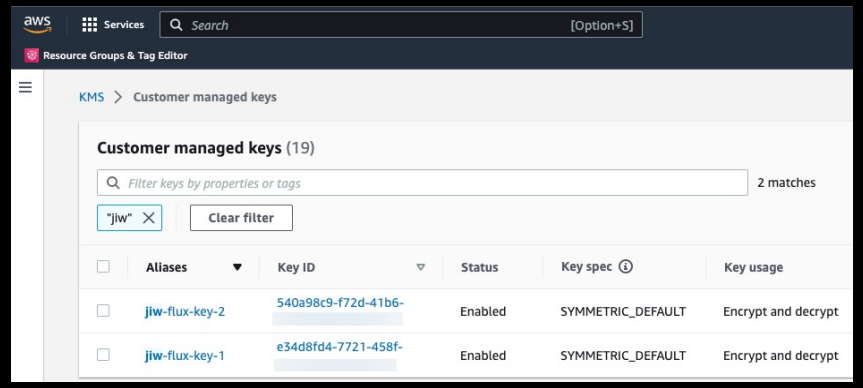
Solution (2) - Flux with AWS Secret



How to setup AWS ?

nimble by krungsri

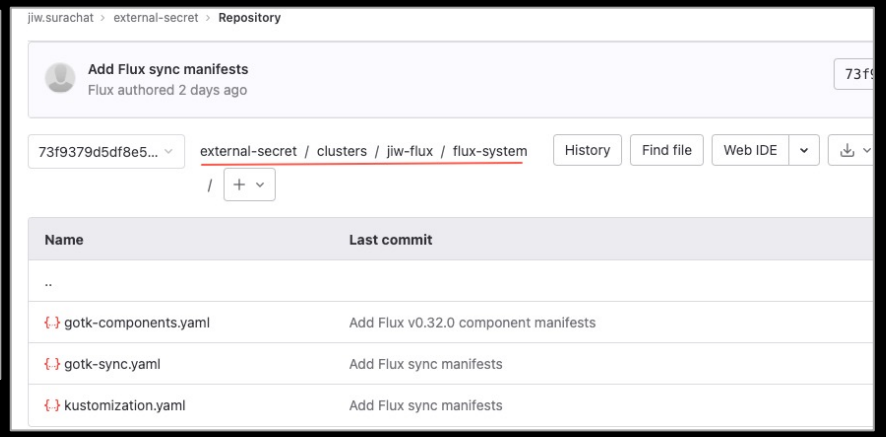
```
aws kms create-key --description "jiw-flux-key-1"
aws kms create-key --description "jiw-flux-key-2"

eksctl utils enable-secrets-encryption --cluster=jiw-flux --key-arn='{ jiw-flux-key-1 } '
-- ** Wait 45 Minute

eksctl utils associate-iam-oidc-provider --cluster= jiw-flux

eksctl utils associate-iam-oidc-provider --cluster=jiw-eks-cluster --approve

aws iam create-policy --policy-name kustomization-controller --policy-document '{
      "Version": "2012-10-17",
      "Statement": [
{
"Action": [
            "kms:Decrypt",
            "kms:DescribeKey"
          ],
          "Effect": "Allow",
"Resource": "{ jiw-flux-key-2 }" }
] }'
```

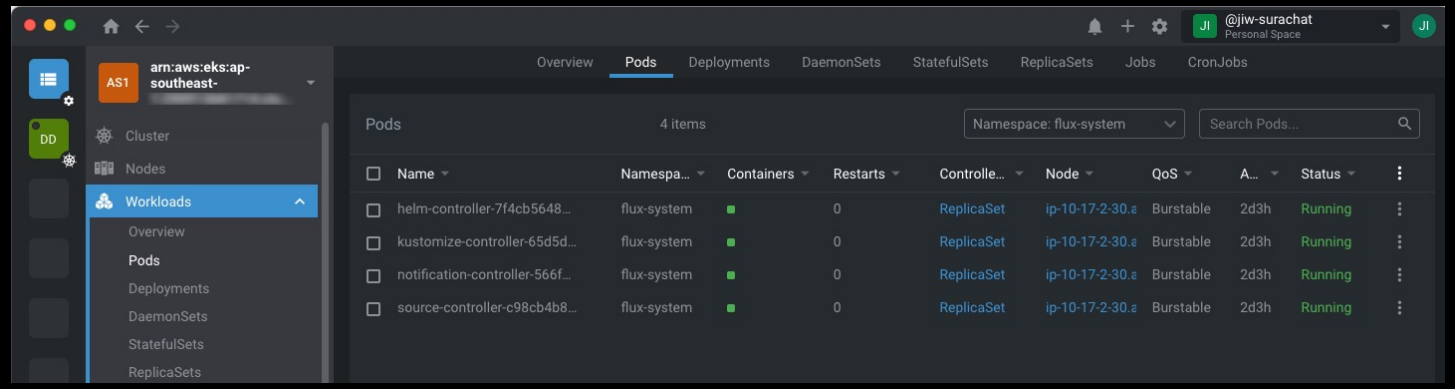


Setup “ Flux ” bootstrap - (GitOps)

```
export GITLAB_USER=jiw.surachat
export GITLAB_TOKEN=glpat-N85-xxxxxx_xxxxx
```

```
flux bootstrap gitlab \
--owner=$GITLAB_USER \
--repository=external-secret \
--branch=main \
--path=./clusters/jiw-flux \
--personal
```





Flux - Infrastructure as code

Application deployment

Application Kustomization / Sync

Flux-system core

Platform/ Security

Demo

Solution 1. Flux with SOPS CLI
Solution 2. Flux with AWS Secret

Q & A