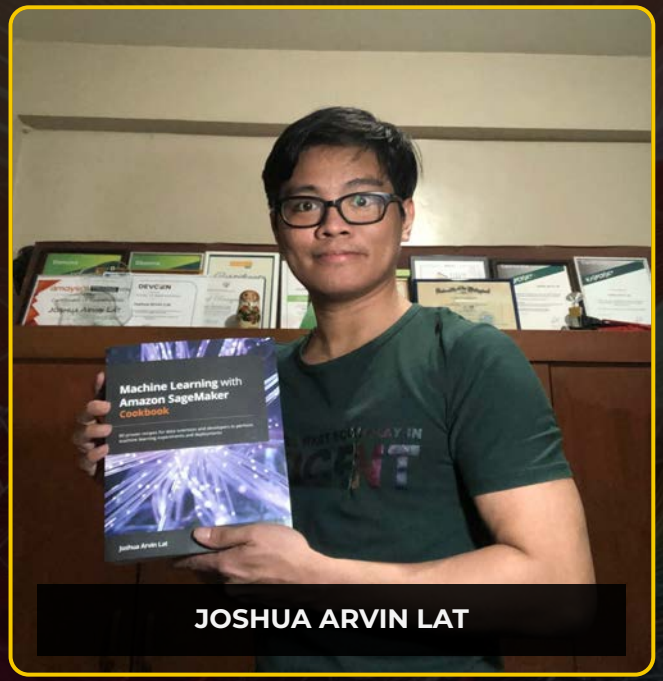
Infrastructure as Code (IaC) Security Best Practices and Strategies

Joshua Arvin Lat



JOSHUA ARVIN LAT

Chief Technology Officer of
NuWorks Interactive Labs

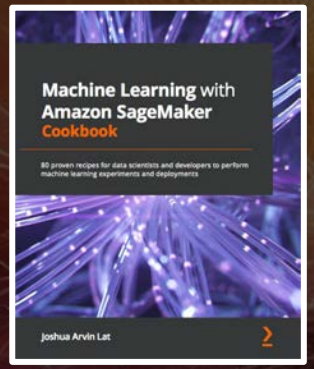
AWS Machine Learning Hero

Orange Boomerang: Digital Leader of the Year 2023 Award Winner 🏆

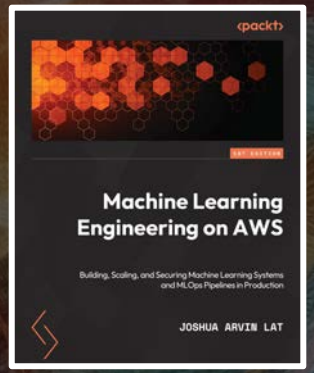
Author of 📖
Machine Learning with Amazon SageMaker Cookbook

Author of 📖
Machine Learning Engineering on AWS

Author of 📖
Building and Automating Penetration Testing Labs in the Cloud

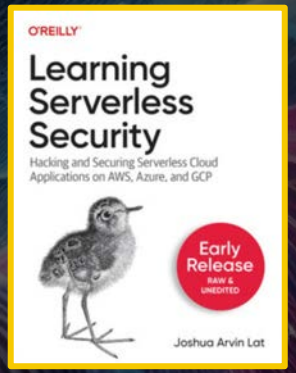


2021



2022

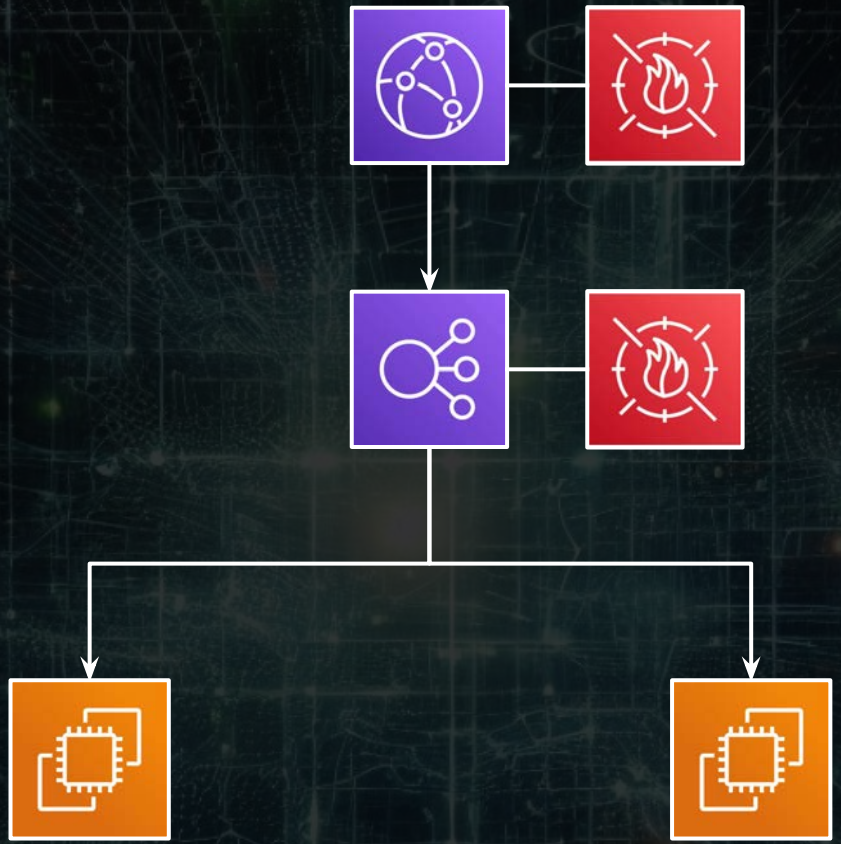
2023

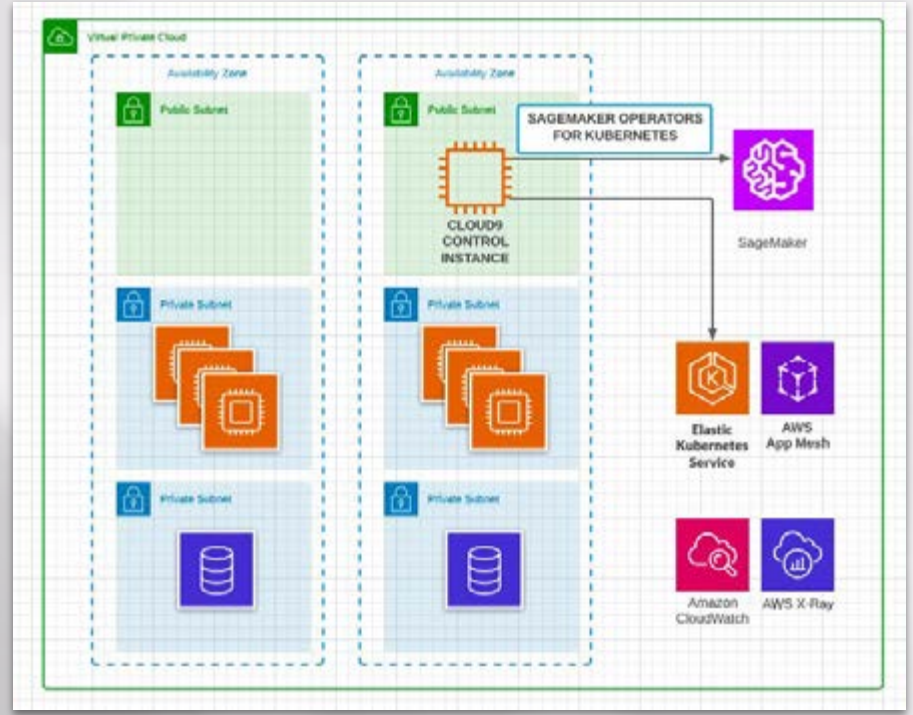


2024

WEB APP

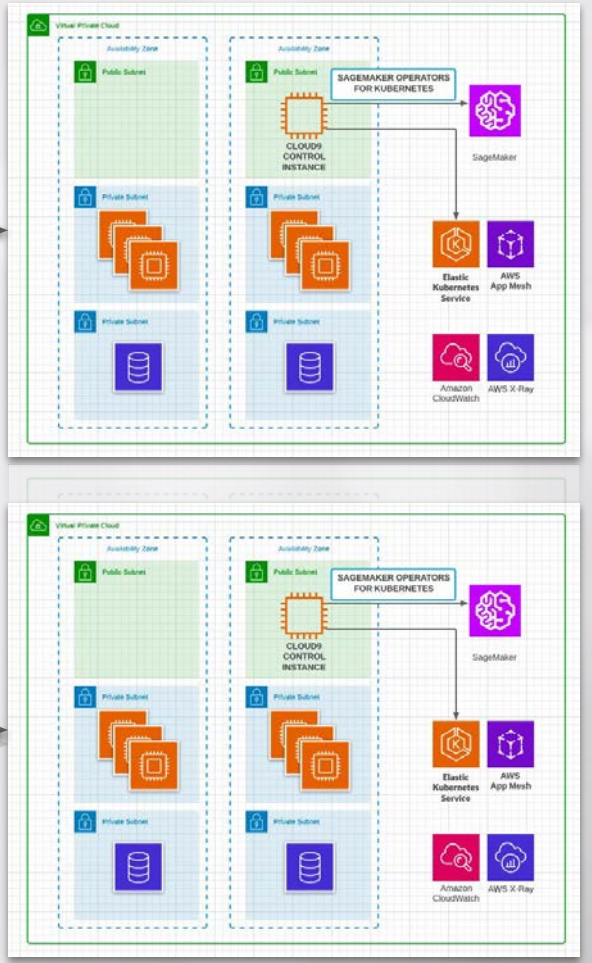
FRONTEND
BACKEND
DATABASE

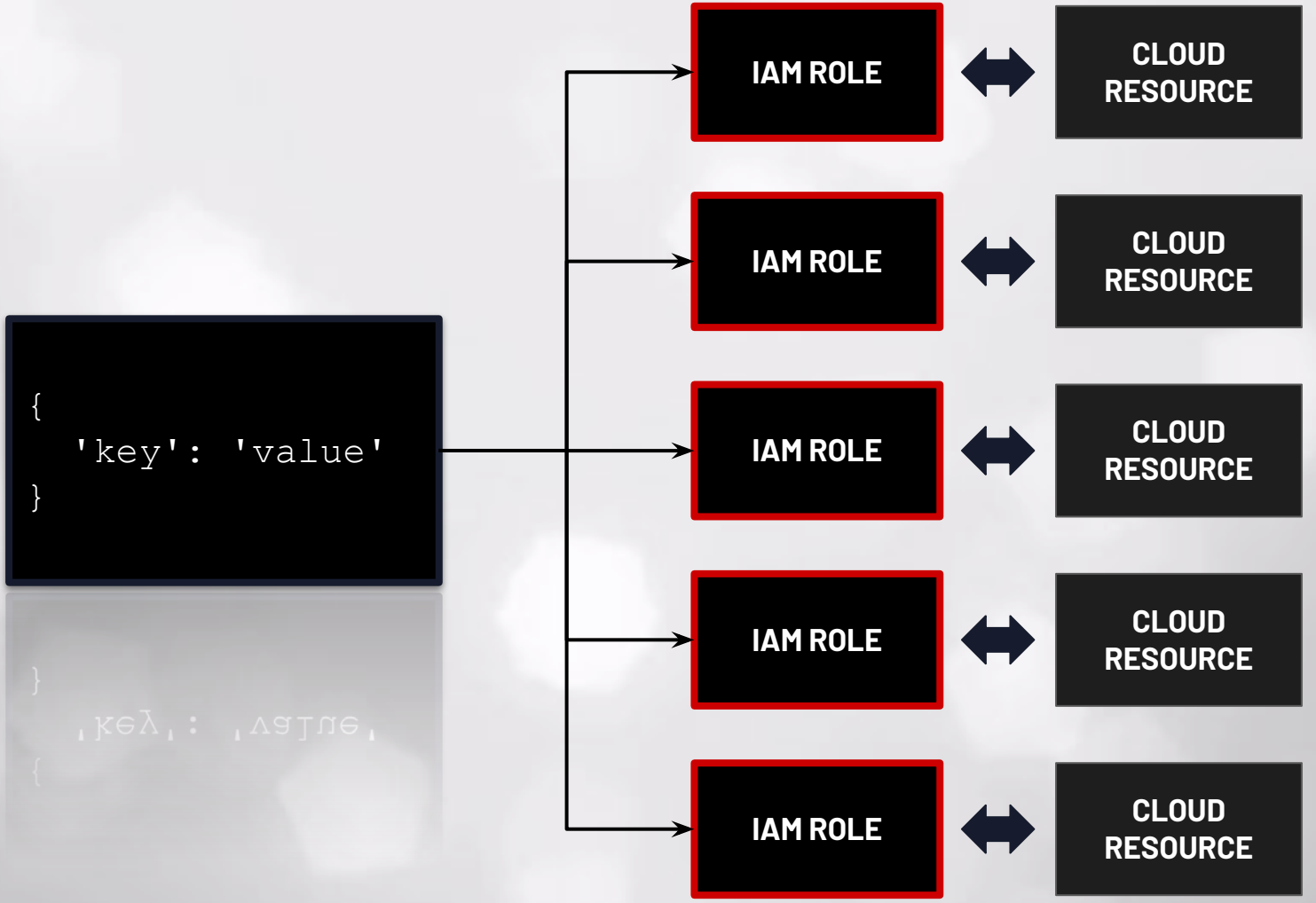



Virtual Private Cloud
Availability Zone
Public Subnet
Private Subnet
Private Subnet
Availability Zone
Public Subnet
SAGEMAKER OPERATORS FOR KUBERNETES
CLOUD9 CONTROL INSTANCE
SageMaker
Private Subnet
Private Subnet
Elastic Kubernetes Service
AWS App Mesh
Amazon CloudWatch
AWS X-Ray

```
{
   'key': 'value'
}
```

```
{
   'key': 'value'
}
```

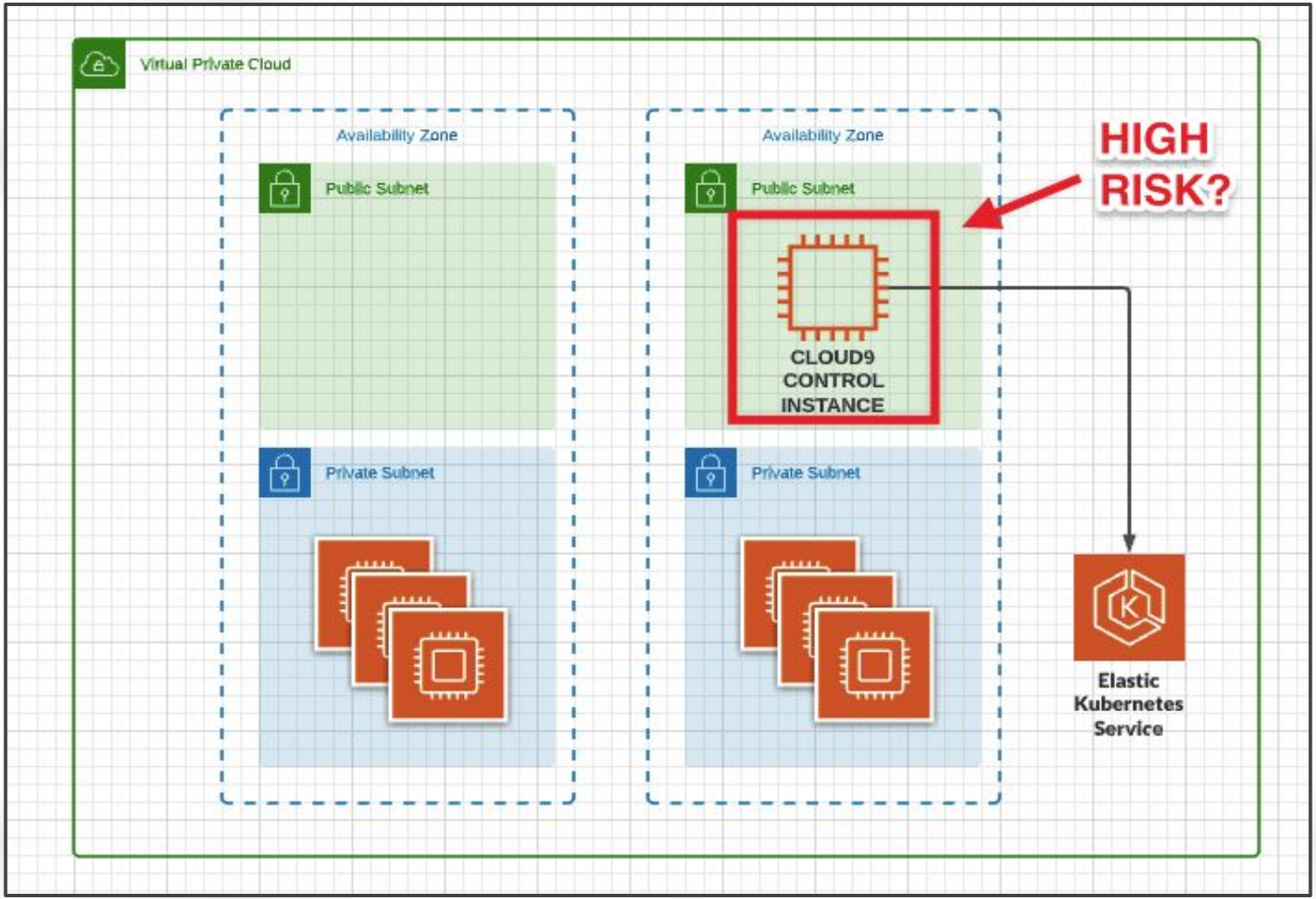

SAGEMAKER OPERATORS FOR KUBERNETES
CLOUD9 CONTROL INSTANCE
SageMaker
Elastic Kubernetes Service
AWS App Mesh
Amazon CloudWatch
AWS X-Ray


{
'key': 'value'
}
IAM ROLE
CLOUD RESOURCE
IAM ROLE
CLOUD RESOURCE
IAM ROLE
CLOUD RESOURCE
IAM ROLE
CLOUD RESOURCE
IAM ROLE
CLOUD RESOURCE

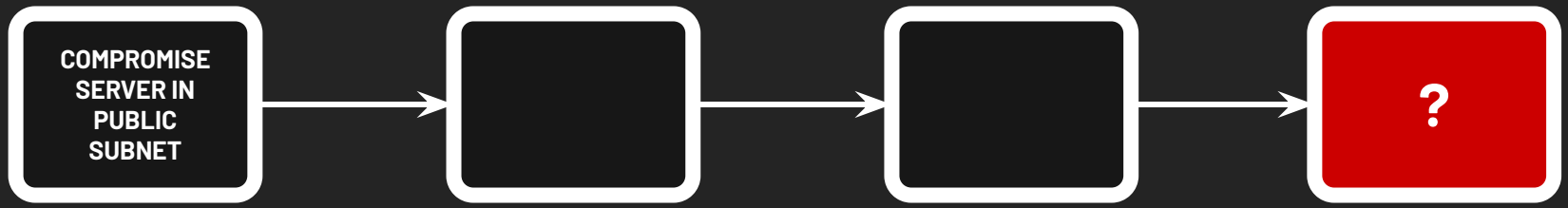
Tag resources properly

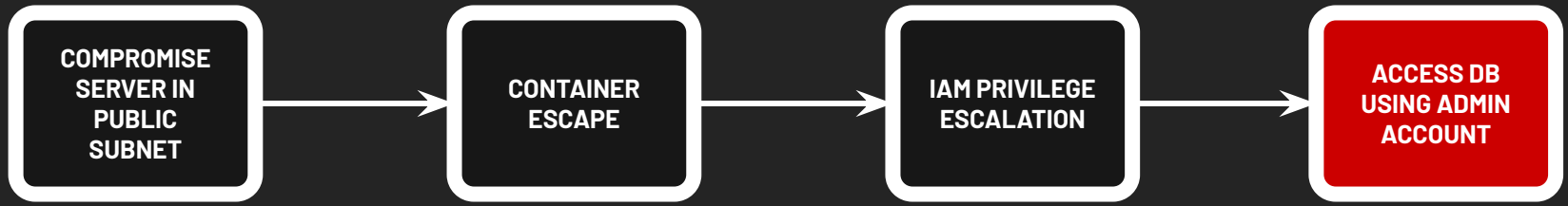
Avoid insecure defaults and regularly check for announcements in cloud platforms

Secret Management & Permission Management

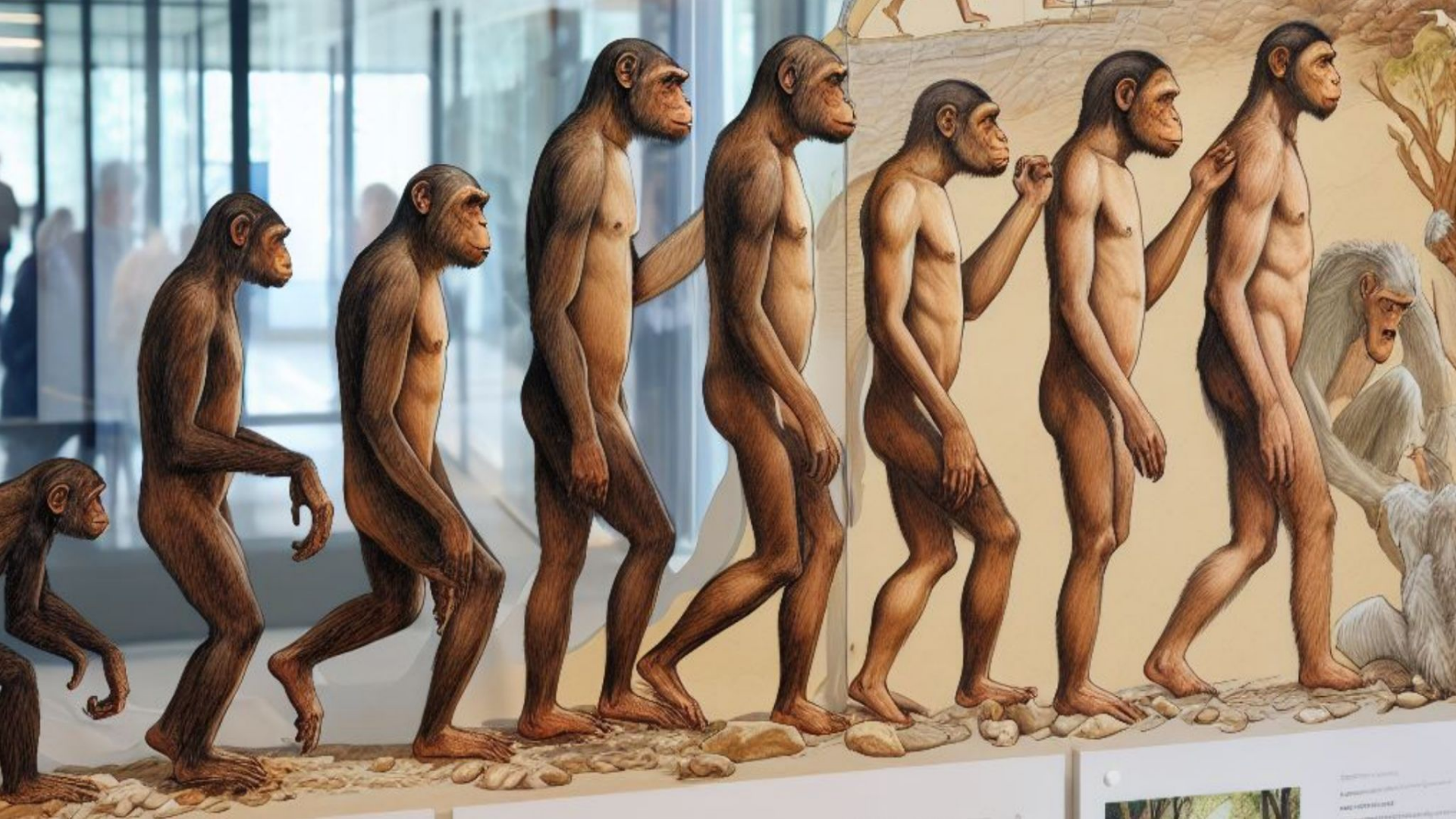

Virtual Private Cloud
Availability Zone
Public Subnet
Private Subnet
Availability Zone
Public Subnet
Private Subnet
HIGH RISK?
CLOUD9 CONTROL INSTANCE
Elastic Kubernetes Service

WHY?

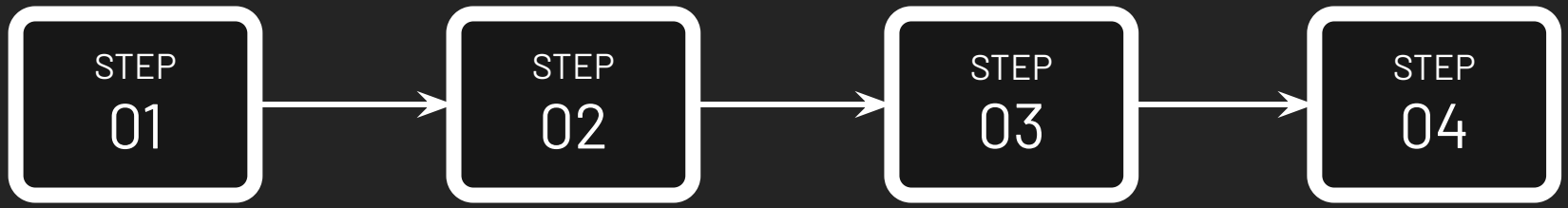

COMPROMISE SERVER IN PUBLIC SUBNET
?


COMPROMISE SERVER IN PUBLIC SUBNET
CONTAINER ESCAPE
IAM PRIVILEGE ESCALATION
ACCESS DB USING ADMIN ACCOUNT

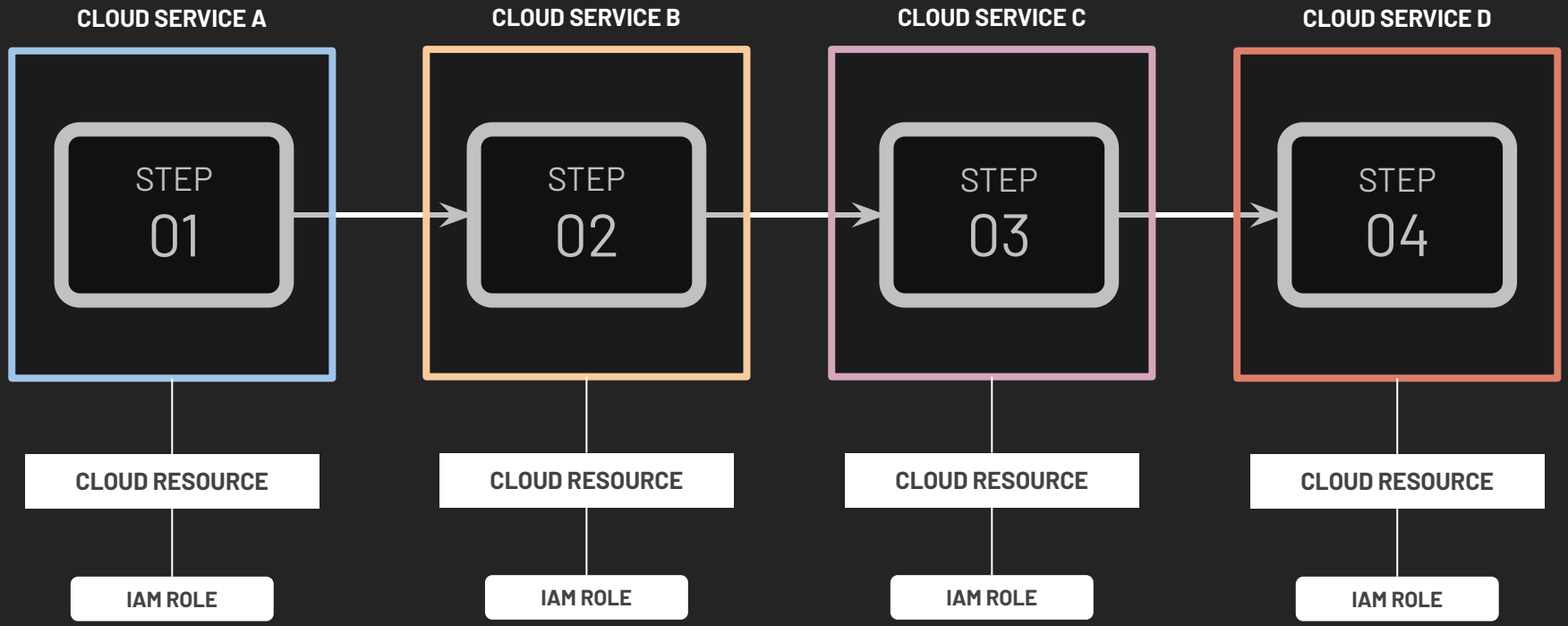
Track and manage changes using version control tools

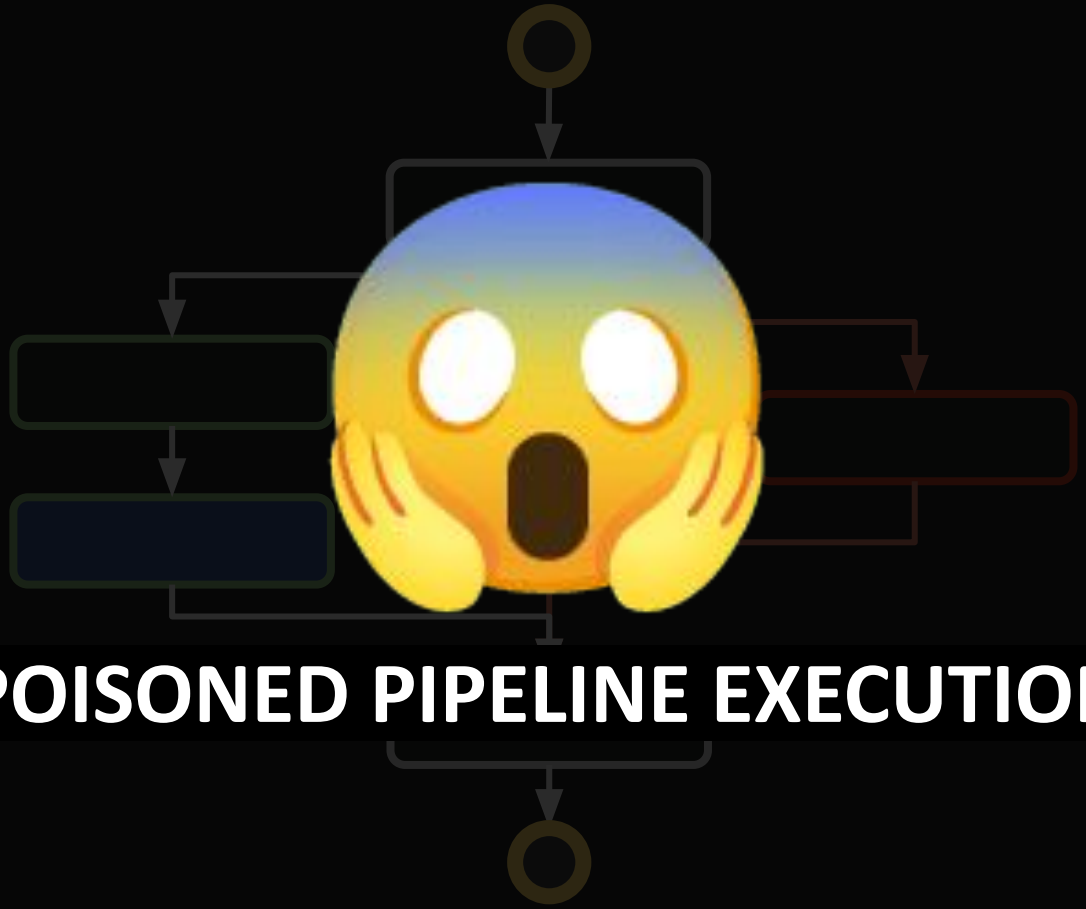


Use pipelines to analyze security vulnerabilities automatically



Be careful when managing resources with IaC in pipelines!


CLOUD SERVICE A
CLOUD SERVICE B
CLOUD SERVICE C
CLOUD SERVICE D
STEP 01
STEP 02
STEP 03
STEP 04
CLOUD RESOURCE
CLOUD RESOURCE
CLOUD RESOURCE
CLOUD RESOURCE
IAM ROLE
IAM ROLE
IAM ROLE
IAM ROLE



POISONED PIPELINE EXECUTION

Protect specific resources from accidental deletion or modification

THE END

Infrastructure as Code (IaC) Security Best Practices and Strategies

Joshua Arvin Lat