Next Generation DevOps - Day 2

Haleh Shahzad
March 2023

Agenda

- **Session Agenda:** 9:05 – 9:15 AM
- **Modules# 5-8 Review:** 9:15 – 10:00 AM
- **Break:** 10:00 – 10:15 AM
- **Assignment #3.1 – Group Work:** 10:15 – 11:30 AM
- **Check Point:** 11:50
- **Lunch:** 12:01 – 01:00 PM (1 Hour)
- **Assignment #3.2 – Group Presentation (12-15 Minutes per Group):** 01:00 – 02:30 PM
- **Break:** 02:30 – 02:45 PM
- **Activity #2 – LAB 2 (Optional)**

Modules# 5-8 Review

9:15 – 10:00 AM (45 Minutes)

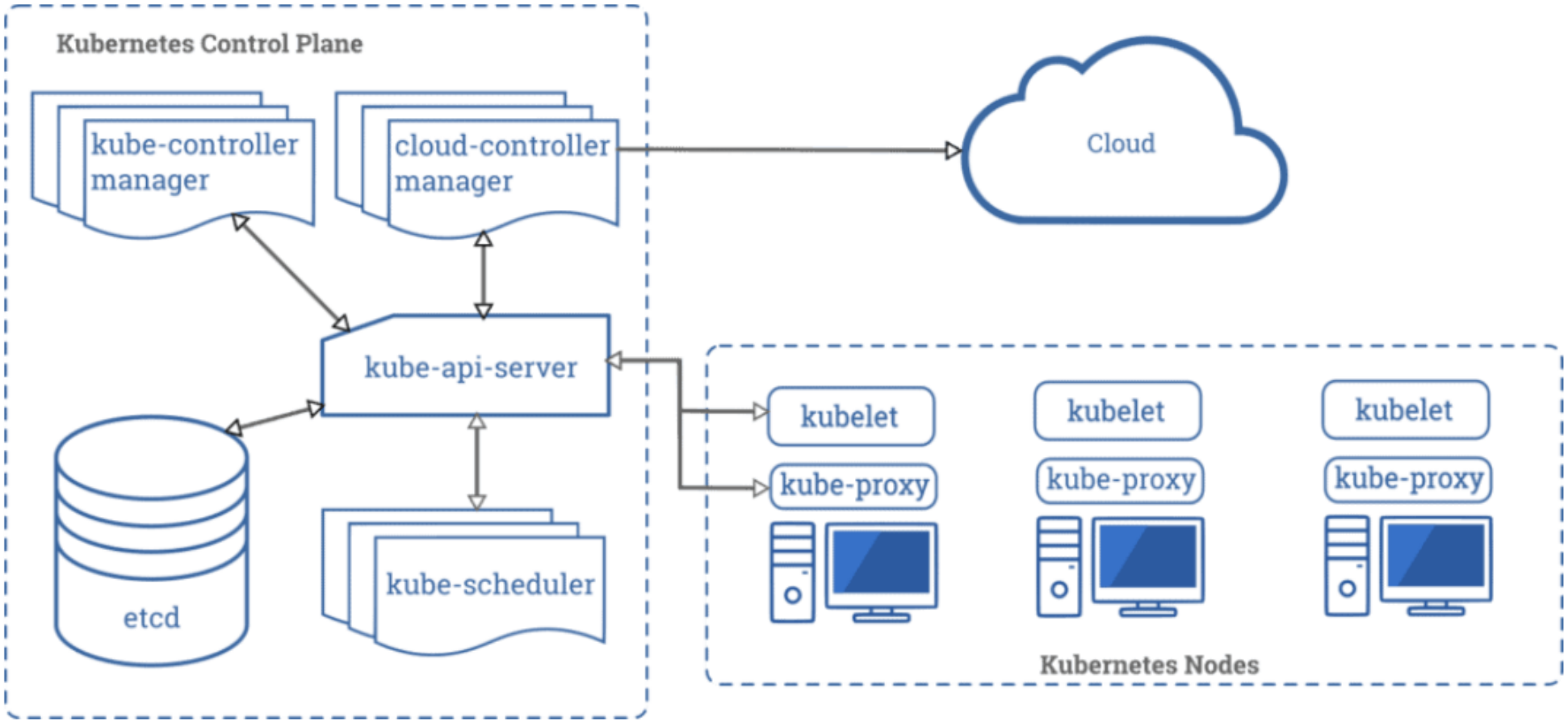
school of continuing studies | YORK U

school of continuing studies | YORK U

Kubernetes (K8s)

school of continuing studies | YORK U

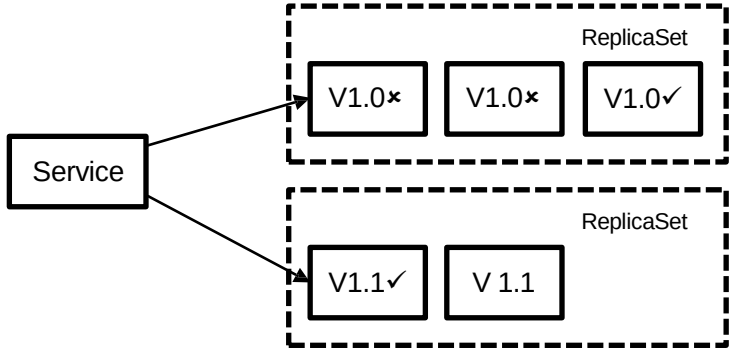
Kubernetes Architecture



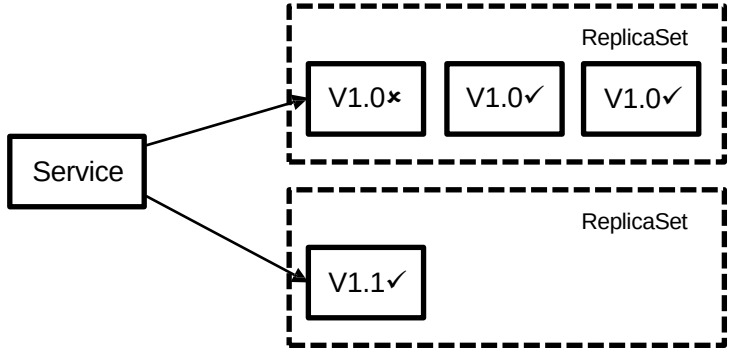
Kubernetes Architecture & Components With Diagram (k21academy.com)

Deployments

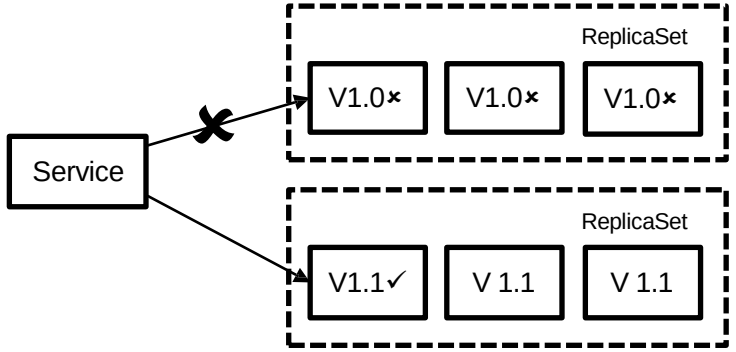
- Rolling Deployment



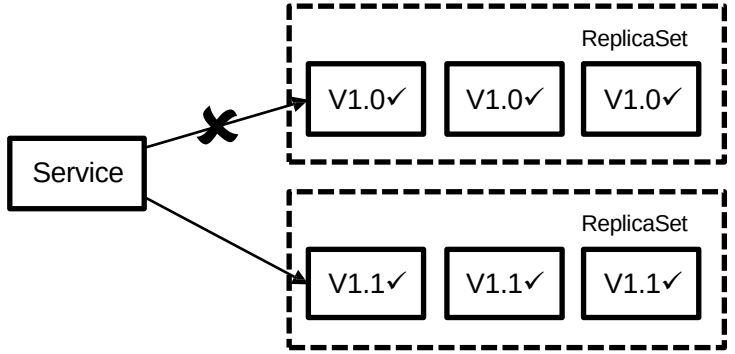
- Canary Release



- Fixed Deployment

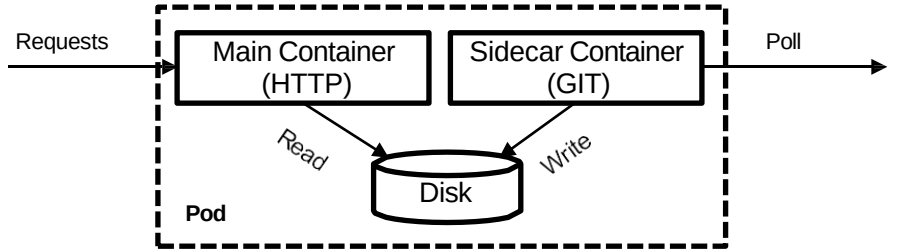


- Blue-Green Release

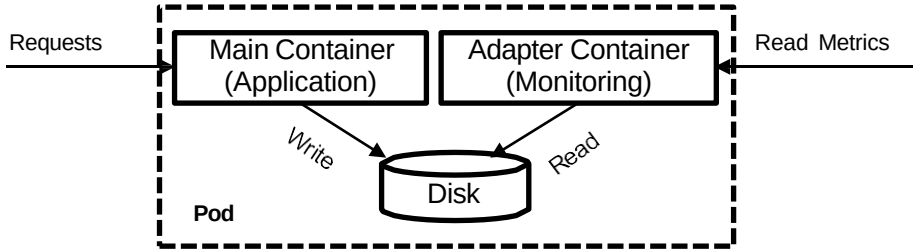


Multi-Container Pods

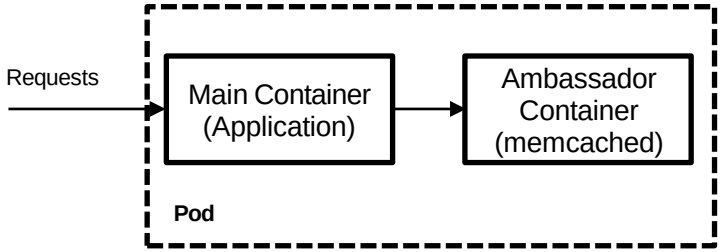
- Sidecar
  - Enhance the application functionality without changing it



- Adapter
  - Decouple access to a container from the outside world



- Ambassador
  - Decouple a container's access to the outside world



GitOps

school of continuing studies | YORK U

GitOps

What?

- Git is the single source of truth

Why?

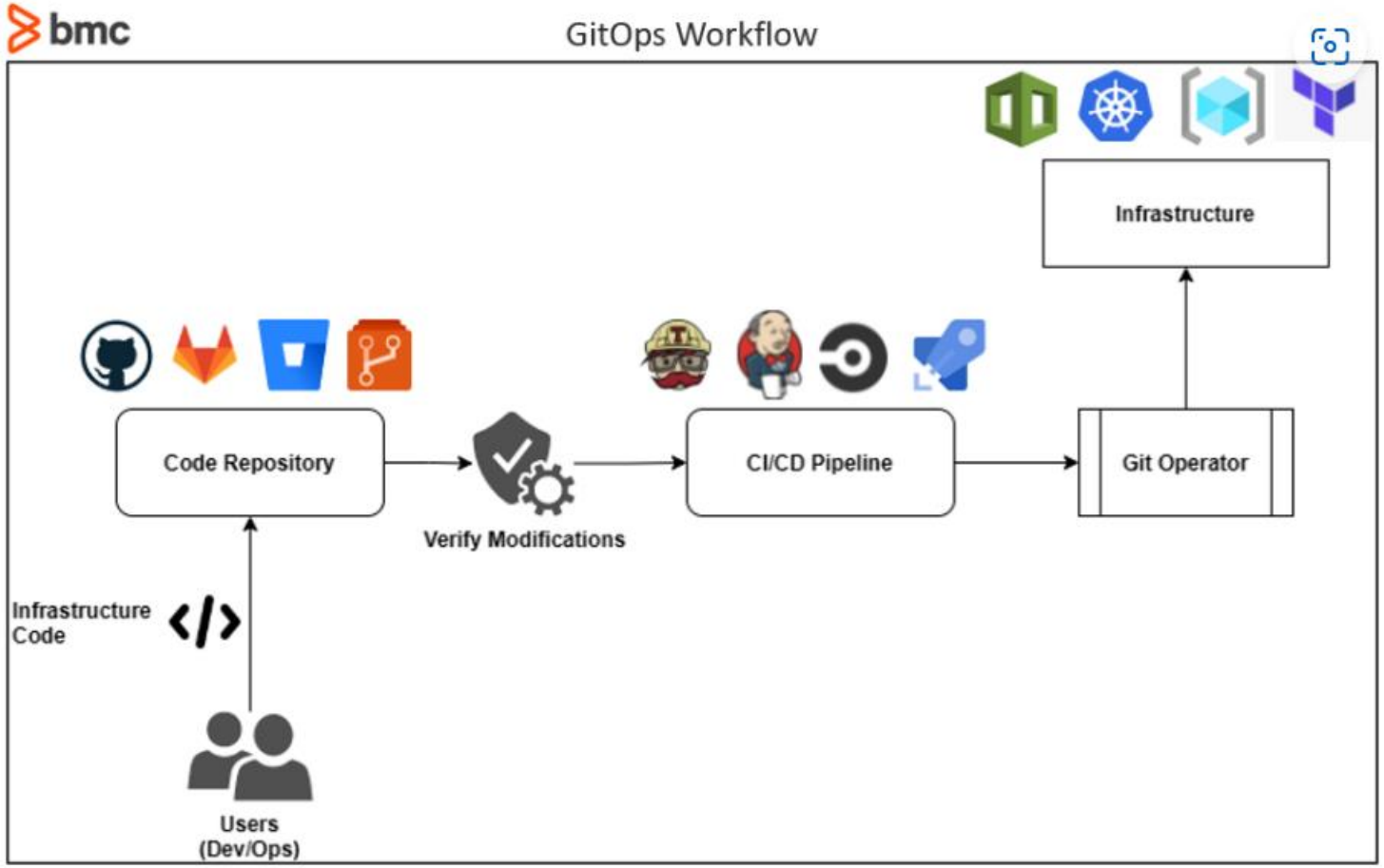
- Simplicity, Easy mental model,
- Declarative, like Kubernetes
- Secure, Easy to monitor – tracking via git history

Principles

- The entire system is described declaratively,
- The canonical desired system state is versioned in Git,
- Approved changes to the desired state are automatically applied to the system,
- And software agents ensure correctness and alert on divergence.

https://n4stack.io/wp-content/uploads/2018/11/Automation-meme.png

GitOps Workflow



Beyond DevOps

school of continuing studies | YORK U

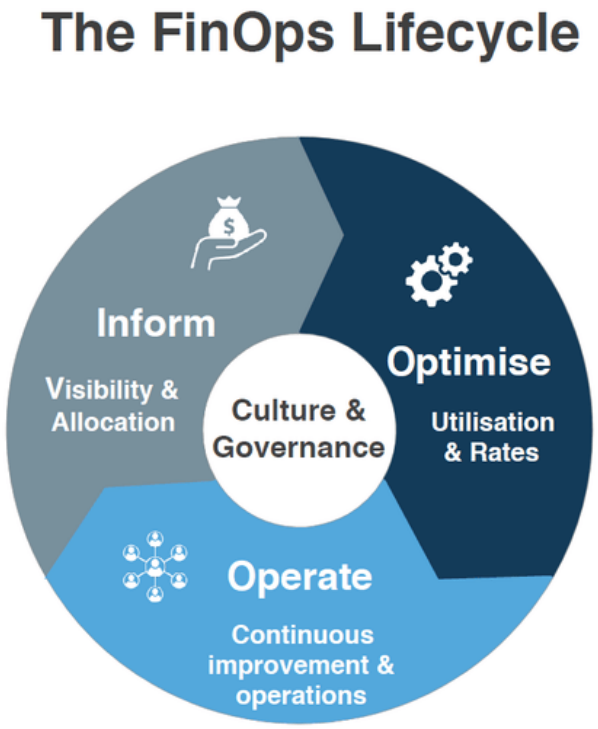
FinOps

Traditional Technology Consumption

- Model
- Engineers as requesters
- Finance as Approvers
- Spend is predictable and static
- Long procurement cycles
- High cost of failure

FinOps is the operating model for cloud spend

- Prescriptive model of actions, best practices and culture
- Enables collaboration with engineer, business & finance teams
- Get the most value out of every dollar spent in cloud



https://research.aimultiple.com/wp-content/uploads/2020/05/finops_cycle.png

MLOps and AIOps

school of continuing studies | YORK U

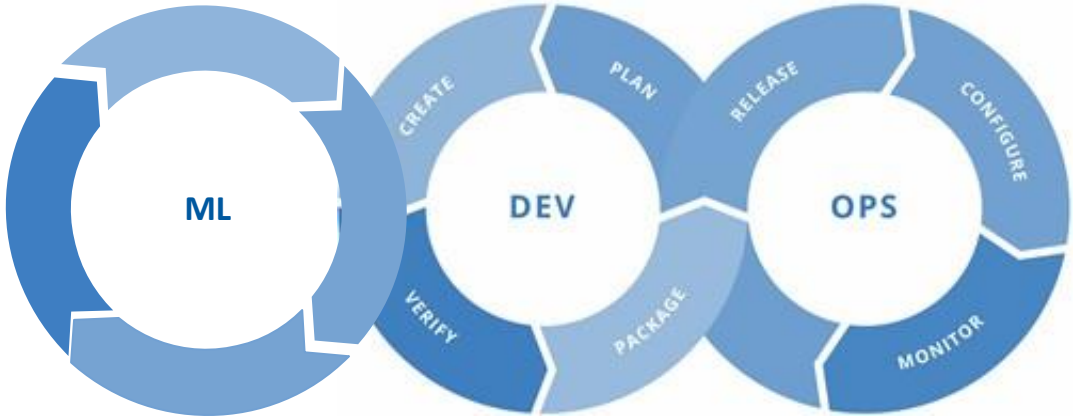
AI, ML & Deep Learning

- Artificial Intelligence (AI)
- Machine Learning (ML)
  - Supervised Learning
  - Unsupervised Learning
  - Semi-Supervised Learning
- Deep Learning

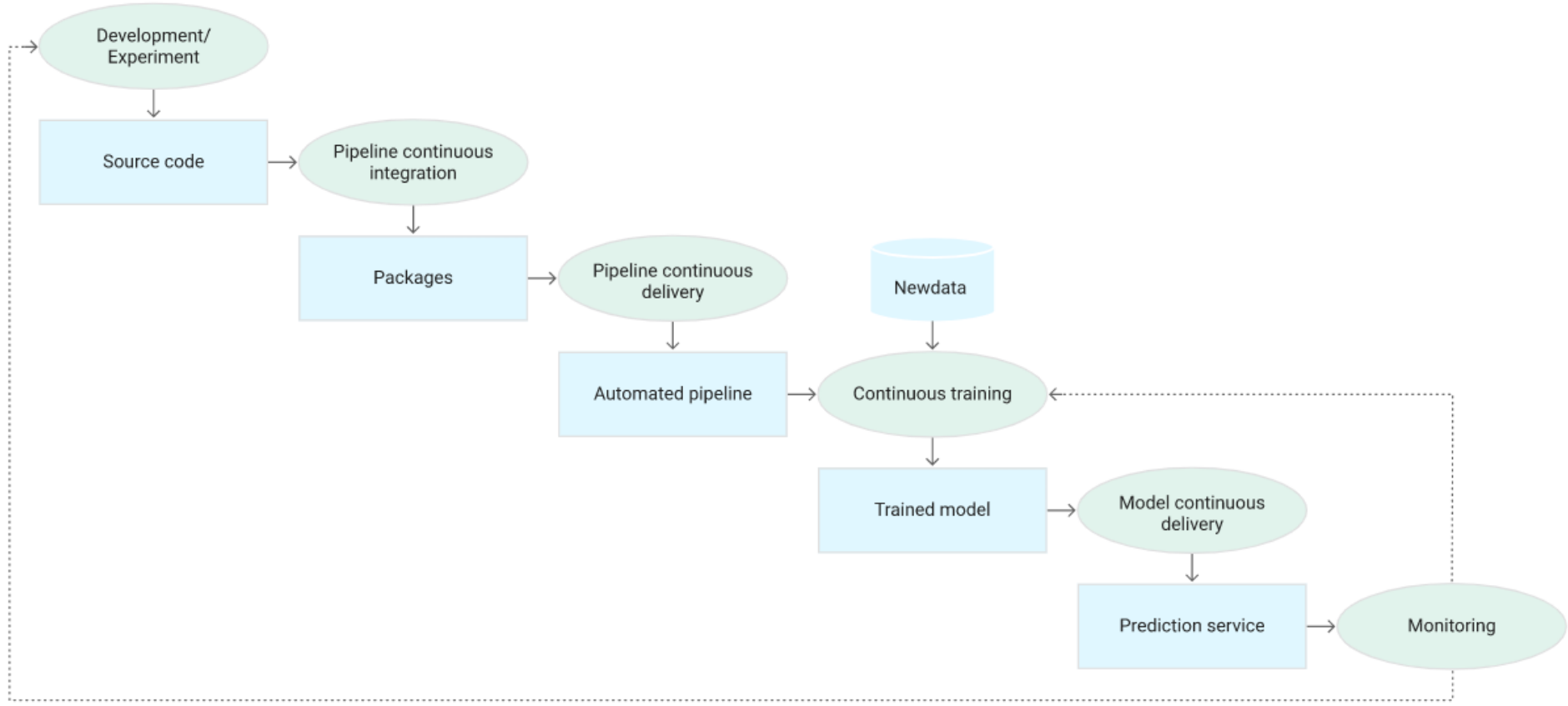
https://www.meme-arsenal.com/memes/bb53262f3b1a625b9c321d3b07946f5d.jpg

MLOps = ML + Dev + Ops

- Experiment
  - Data Acquisition
  - Business Understanding
  - Initial Modeling
- Develop
  - Modeling + Testing
  - Continuous Integration
  - Continuous Deployment
- Operate
  - Continuous Delivery
  - Data Feedback Loop
  - System + Model Monitoring

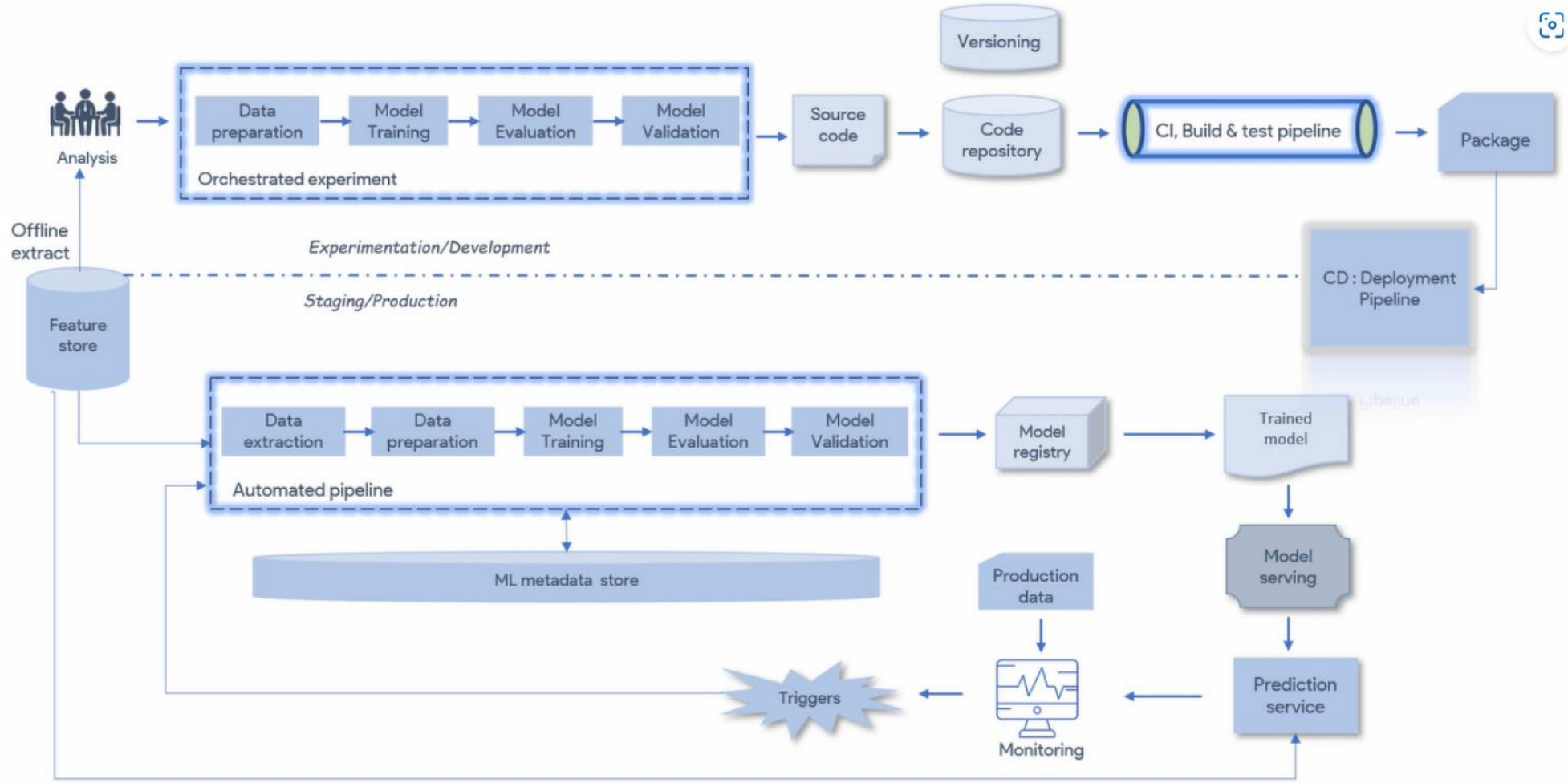


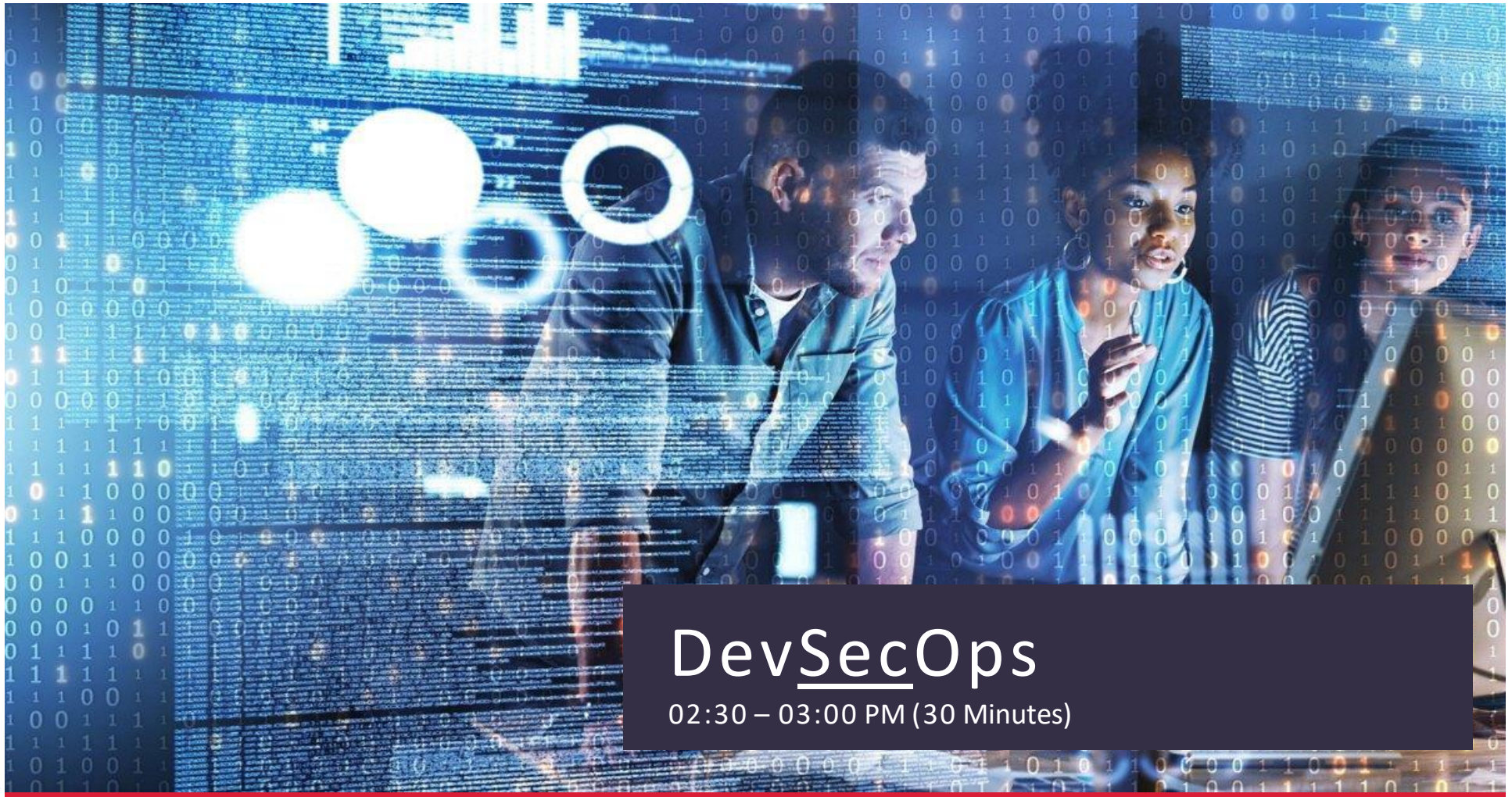
Stages of the CI/CD automated ML pipeline



https://cloud.google.com/architecture/images/mlops -continuous-delivery-and-automation-pipelines-in-machine-learning-5-stages.svg

Stages of the CI/CD automated ML pipeline





DevSecOps

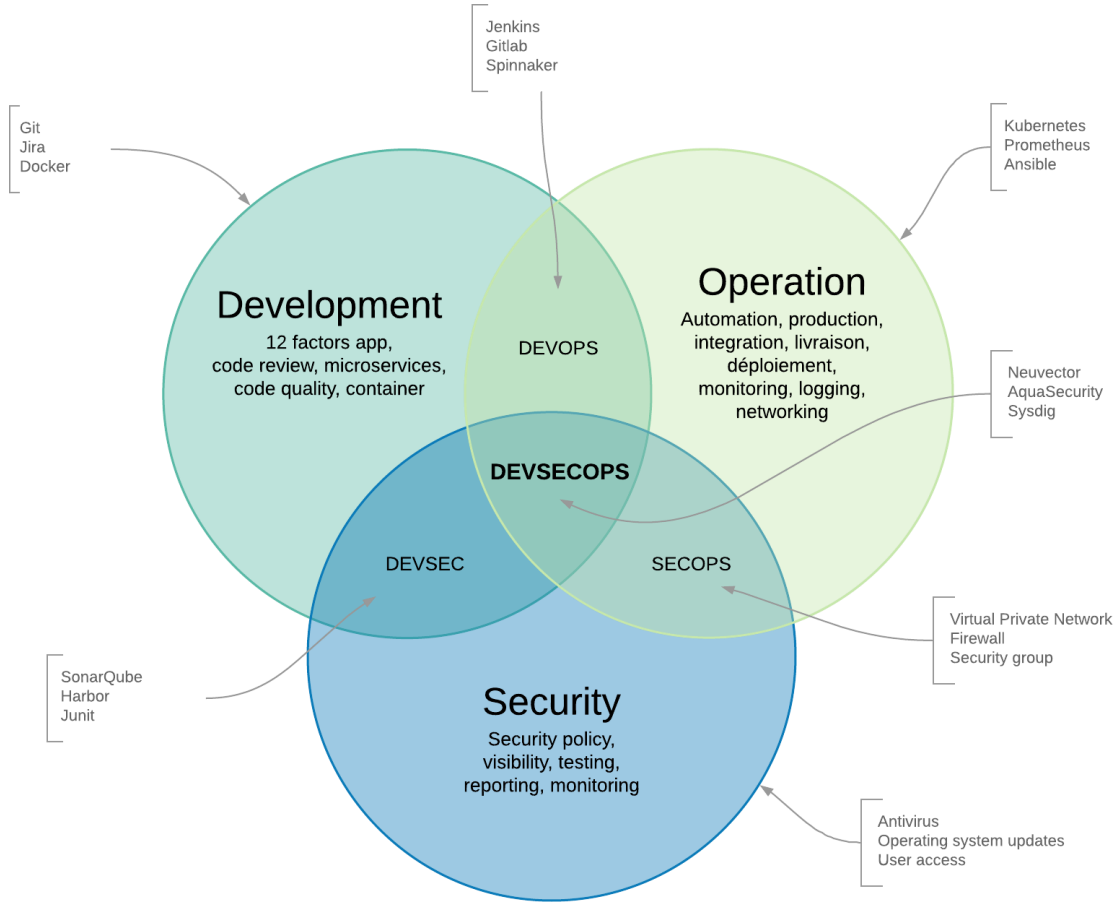
02:30 – 03:00 PM (30 Minutes)

https://sloanreview.mit.edu/wp-content/uploads/2020/05/GEN-Wilson-Cybersecurity-Human-Performance-2400x1260-3-1200x630.jpg

school of continuing studies | YORK U

DevSecOps

- Built-in security and is not applied as an afterthought.
- Automation of security and implementation of security at scale.
- Enable speed and agility, but not at the expense of validating security.

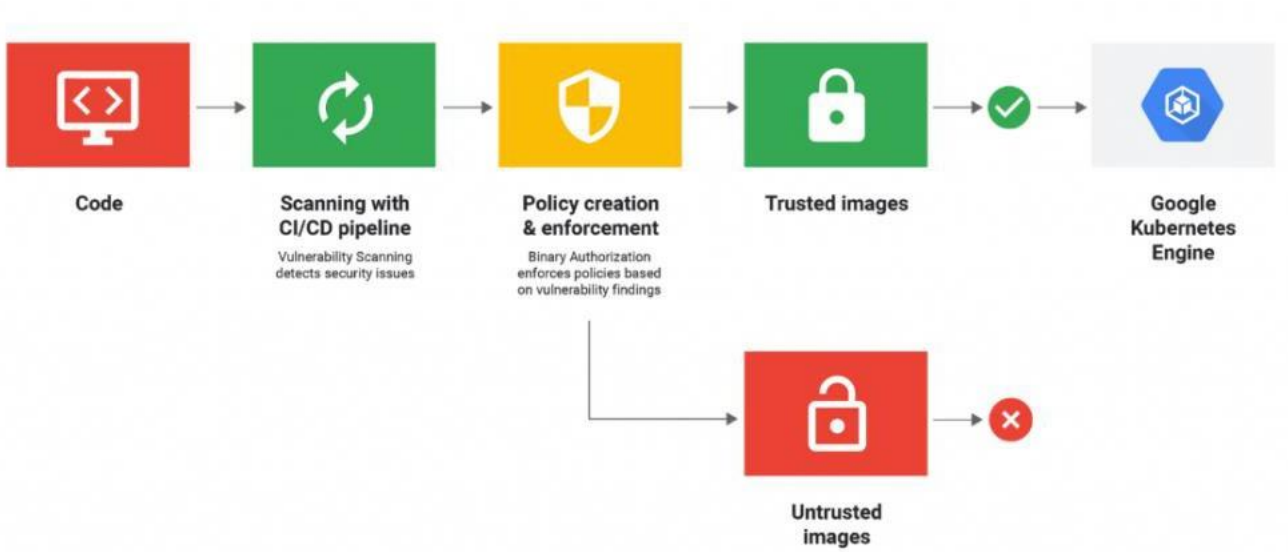


https://miro.medium.com/max/1838/1*l1mvS4zTPn3k2T7auz3qDg.png

DevSecOps and CI/CD

A DevSecOps practice needs to be embedded with every step of the CI/CD pipeline.

- Code: Scan for Secrets
- Build: Tag Security Artifacts
- Test: Test Security meets Standards
- Deploy and Register Security Components
- Provision
- Monitor: Monitor Security Standards



https://cdn.thenewstack.io/media/2018/10/3c246f6f -google-cicd-1024x498.png

K8s Security

Kubernetes security is based on the 4C's

- Cloud or Corporate Datacenter/Colocation facility
- Cluster
- Container
- Code

Top K8s security vulnerabilities during build

- Code from untrusted registries
- Bloated base image

Top K8s security vulnerabilities during deployment

- Granting unnecessary privileges
- Failure to isolate applications in the cluster
- Unauthorized access

Top K8s security vulnerabilities during runtime

- Infrastructure attacks
- Complexity

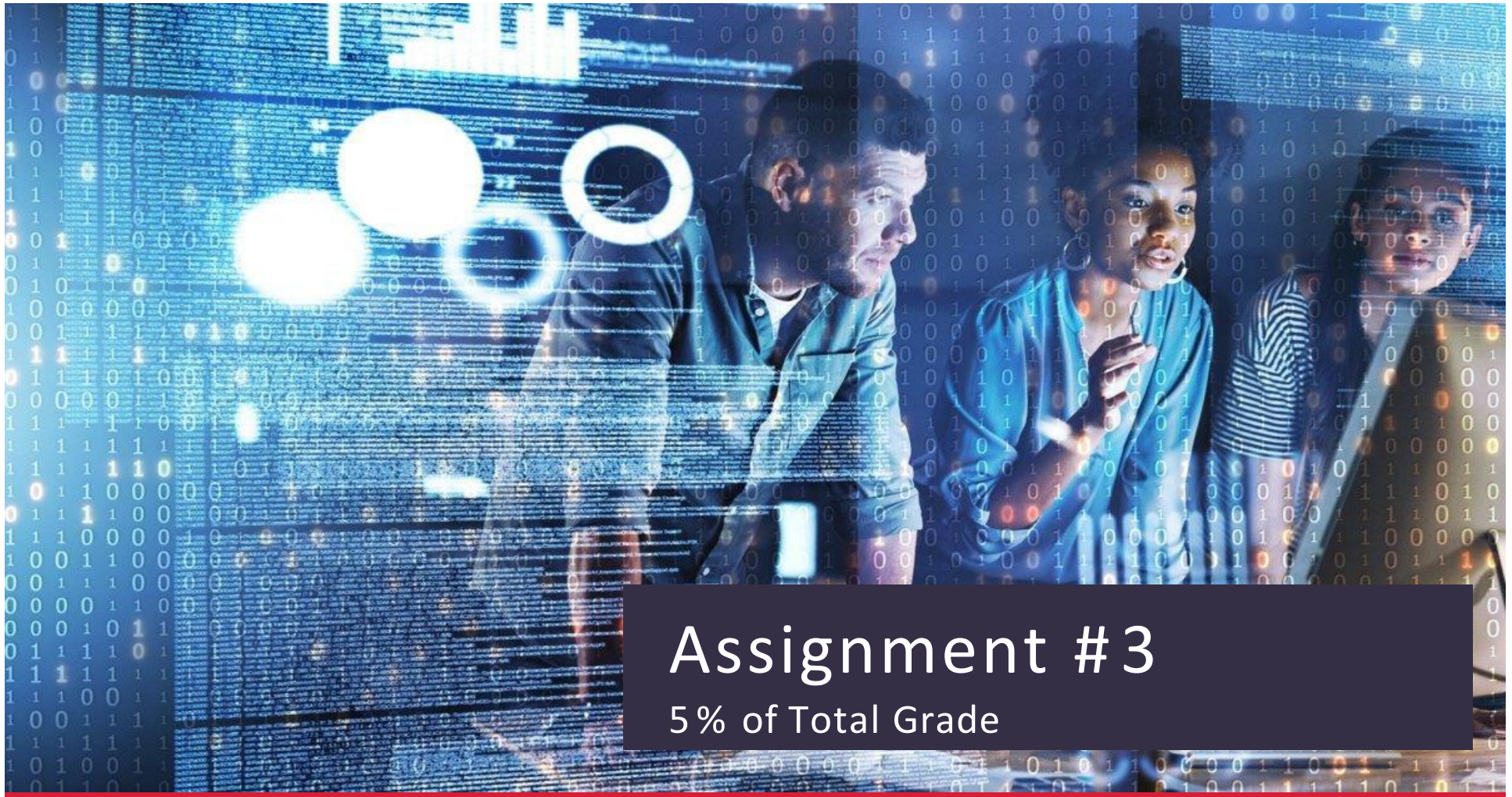
https://anchore.com/wp-content/uploads/2019/04/Screen-Shot-2019-04-01-at-4.32.42-PM.png

Break

10:00 – 10:15 AM
(15 Minutes)

https://i.ytimg.com/vi/EY8EsOY8Naw/maxresdefault.jpg

school of continuing studies | YORK U



Assignment #3

5% of Total Grade

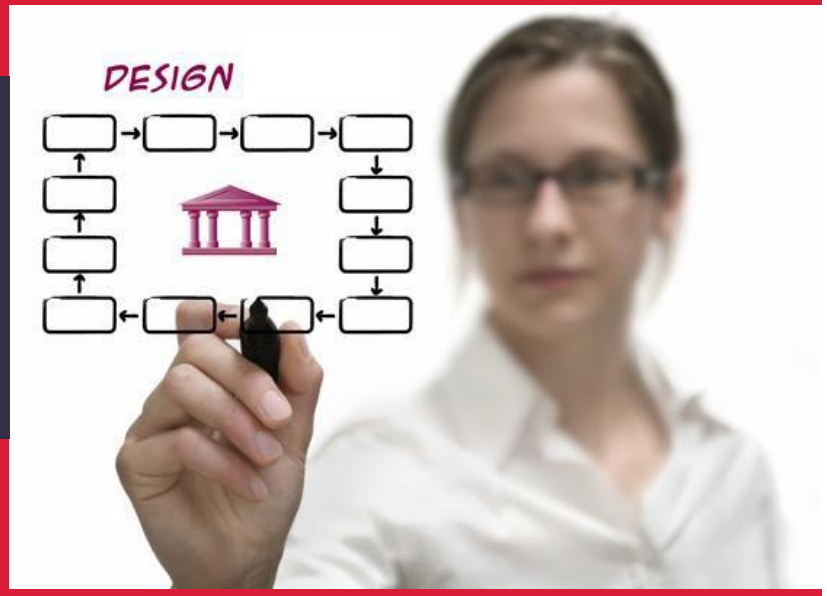
https://sloanreview.mit.edu/wp-content/uploads/2020/05/GEN-Wilson-Cybersecurity-Human-Performance-2400x1260-3-1200x630.jpg

school of continuing studies | YORK U

school of continuing studies | YORK U

Assignment #3.1

10:15 – 11:30 AM (1.15 Hour)



school of continuing studies | YORK U

school of continuing studies | YORK U

Assignment #3.1 – Group Work

You work for a startup company and have been asked to present the following as a group:

- DevOps and emerging technologies such as (Data and Analytics, Machines Learning, Artificial Intelligence)
- A flow diagram for a CI/CD Pipeline using Public Cloud Providers (AWS or Azure or GCP) Managed Services

Guidelines

- No more than 15 slides per group.
- Time to present 12-15 minutes per group.
- Each member must present at least 1-2 slides.
- You should nominate a lead, who combine the slides and share screen during the presentation.

Assignment #3.1 – Group Work

You work for a startup company and have been asked to present the following as a group:

- DevOps and emerging technologies such as (Data and Analytics, Machines Learning, Artificial Intelligence)
- A flow diagram for a CI/CD Pipeline using Public Cloud Providers (AWS or Azure or GCP) Managed Services

Guidelines

- No more than 15 slides per group.
- Time to present 12-15 minutes per group.
- Each member must present at least 1-2 slides.
- You should nominate a lead, who combine the slides and share screen during the presentation.

Checkpoint

school of continuing studies | YORK U

Lunch Break

12:01 – 01:00 PM (1 Hour)

https://imagesawe.s3.amazonaws.com/articles/2020/09/dash_diet_tips.jpg

school of continuing studies | YORK U

Group Presentation

Assignment #3.2

01:00 – 02:15 PM (1–1.15 Hour)

school of continuing studies | YORK U

school of continuing studies | YORK U

Break

https://www.facebook.com/pg/fifeteenminute/posts/

school of continuing studies | YORK U

Activity #2

Optional-Not graded

school of continuing studies | YORK U

school of continuing studies | YORK UNIVERSITÉ UNIVERSITY

Activity #2 – LAB 2 – K8s Secrets

- Great for Access Keys, Passwords, Tokens, etc.
- On a Node that needs them, they are stored in memory (never to physical memory).
  - Note: root users on the node can still easily access the secret within the container through the filesystem as long as that container is alive.
- Only loaded as-needed by pods.
- Easy authorization policy with RBAC.
- Not great for non-sensitive or lengthy configs, documents, large files.
  - Use ConfigMaps or other storage.
- The kubernetes docs on Secrets are great.

https://kubernetes.io/docs/concepts/configuration/secret/

https://sloanreview.mit.edu/wp-content/uploads/2020/05/GEN-Wilson-Cybersecurity-Human-Performance-2400x1260-3-1200x630.jpg

Activity #2 – LAB 2 – K8s Secrets (Cont.)

- Make Secrets

  kubectl create secret generic sensitive-key
  --from-file=./sensitive.key --namespace=app-sensitive

- Use Secrets in Pods

```
apiVersion: v1
kind: Pod
metadata:
  name: pod-with-secret
  namespace: app-sensitive
spec:
  containers:
  - image: gcr.io/org/app
    name: app-with-secret
  volumeMounts:
  - name: keys
    mountPath: "/etc/key"
    readOnly: true
  volumes:
  - name: keys
    secret:
      secretName: sensitive-key
```

https://sloanreview.mit.edu/wp-content/uploads/2020/05/GEN-Wilson-Cybersecurity-Human-Performance-2400x1260-3-1200x630.jpg

Questions?

Resources - Networking 101

- Layers of OSI Model link
- TCP/IP Model link
- Introduction of Classful IP Addressing link
- IP Addressing | Classless Addressing link
- Classless Inter Domain Routing (CIDR) link
- Classful Vs Classless Addressing link
- Domain Name Server (DNS) in Application Layer link
- What is DNS (Domain Name System)? **(Video)** link
- Load Balancing link
- Virtual Networking Explained **(Video)** link
- NAT and Firewall Explained **(Video)** link
- Content Delivery Networks (CDNs) link
- What is a Content Delivery Network (CDN)? **(Video)** link

https://images.idgesg.net/images/article/2017/10/cloud_computing_connections__laptops_thinkstock_533215383_3x2-100740704-large.jpg?auto=webp