What is CI/CD

CONTINUOUS INTEGRATION (CI)

The practice of merging all developers' working copies to a shared mainline several times a day.

CONTINUOUS DEPLOYMENT (CD)

A software engineering approach in which the value is delivered frequently through automated deployments.

Why do we need CI/CD?

- Faster and More Frequent Production Deployments
  - CI/CD employs tools and practices that facilitate the release of value-generating features quickly and frequently resulting in a significant increase in revenue
- Deploy to Production Without Manual Checks
  - Avoids error-prone manual checks done by humans before deployment in favor of automated checks and deployments that helps our product features reach market in less time boosting revenue.

Why do we need CI/CD?

- Catch Compile Errors After Merge
  - Issues that emerge upon integrating new developer code to existing code base force our teams to spend more time resolving these issues instead of focusing on product features.
  - CI/CD makes identifying such integration issues easier by isolating the source of the issues and referring each issues to the responsible team member resulting in faster issue resolutions cutting down the time and cost spent on identifying and solving merging issues.

Why do we need CI/CD?

- Catch Unit Test Failures
  - Unit tests help ensure our code is ready for production and functions as expected. Using CI/CD to automate unit tests enhances the speed and frequency at which unit tests are performed against our production code increasing the quality of our software with less or no bugs. This way CI/CD will help us avoid costs related to fixing bugs on production and manual testing.

Why do we need CI/CD?

- Detect Security Vulnerabilities
  - There’s a growing risk of cyber attacks and cyber crimes that any reputable software product should guard against to protect its users. This responsibility cannot be left to manual human check-ups for security holes in our own system or a third party software our software depends on. CI/CD will save us a huge embarrassment and cost by detecting and reporting security holes in our software as soon as they appear.