Our project, DiDx - (Defence in Depth Extended), is a multilayer cybersecurity simulation project. The goal of this project is to mimic a real-world infrastructure by implementing cybersecurity practices and tools. It is an infrastructure monitoring and security toolset that integrates multiple open-source solutions to build a robust, secure, and scalable environment.

The project includes a web-based application deployed using Kubernetes for container orchestration, with automated deployment and updates through CI/CD pipelines to ensure zero downtime.On the master node, an Intrusion Detection System (IDS) is deployed for enhanced protection.

A perimeter firewall provides network security, and Fail2Ban with iptables is implemented on every server to enhance server-level security.

Network segmentation is applied to differentiate between network zones, and the systems are continuously monitored using alert logs, metrics monitoring, and creative, easy-to-understand dashboards that facilitate monitoring and alerting via email notifications.

The primary objective of this project is to demonstrate a defense-in-depth strategy by securing network layers, monitoring system health, automating deployment pipelines, and analyzing security threats in real-time. It showcases the practical implementation of modern cloud-native technologies combined with cybersecurity tools to create a resilient infrastructure.