Project 3 - Fake architecture orchestrator

Cybersecurity experts have recently proposed using defensive deception as a means to leverage the information asymmetry typically enjoyed by attackers as a tool for defenders. By creating fake services and components that appear as valuable targets to attackers, defenders can divert the attacker's attention and resources away from critical assets. Attackers might spend time and effort trying to compromise these fake elements, leaving less capacity to target actual valuable assets**. The goal of this project is to easily instantiate a complex "fake" infrastructure from an architectural diagram.**

Specification

* Detect the type and number of components in a diagram
* It must be possible to associate (via configuration) a docker image to each type of component in the diagram
* The diagram can be provided in one of the following ways:
  + standard image: use a computer vision technique to classify and count the different type of resources in an image. (You can use premade models to speed up the task for example <https://github.com/ultralytics/yolov5/wiki/Train-Custom-Data>)
  + provide an architectural diagram using draw.io and leverage the xml export to parse the structure of the diagram (<https://www.drawio.com/doc/faq/export-to-xml>)
* Generate the terraform plan required to instantiate the desired architecture using the provided docker images as a base for each resource