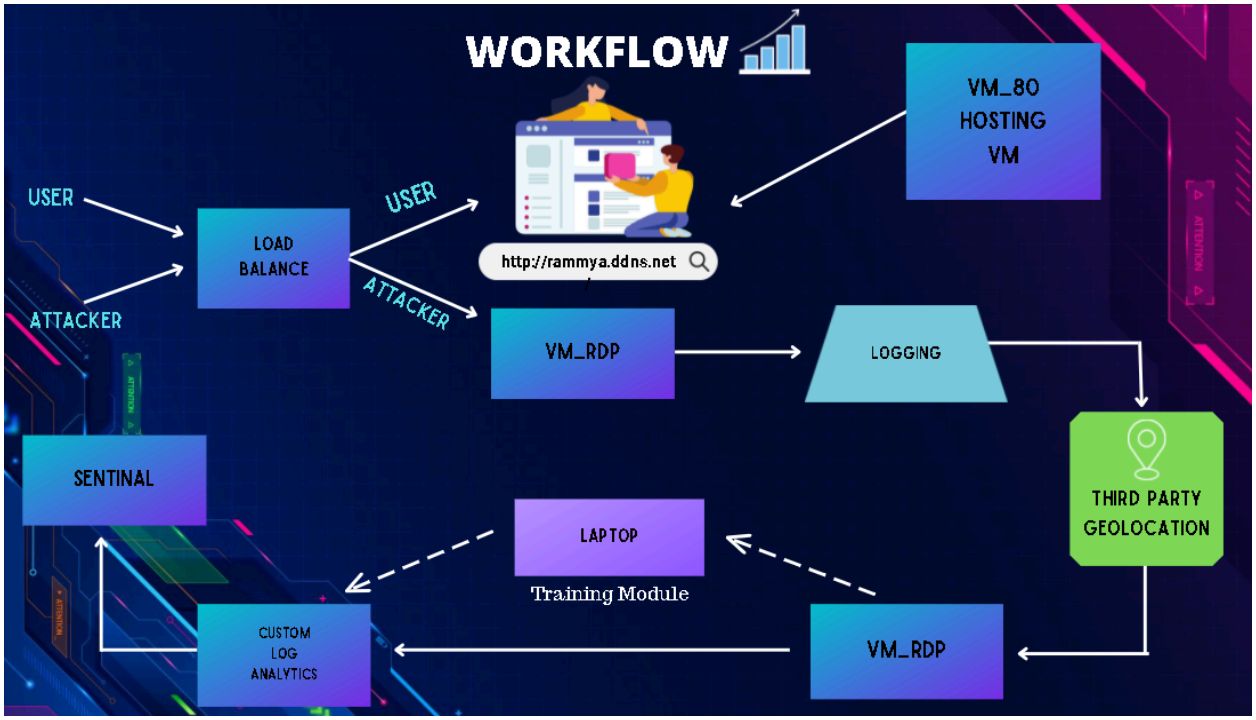

Our project has 2 modules,made to effective accomplish two sets of goals

1. To **secure client website** but effectively understanding and differentiating the **network** coming on the website using the **Load balancer Module**
2. To **visualize** the data coming in and parsing it out in **graphical manner** so the non technical and technical folks can effectively understand our **networks** and all the **malicious traffic** on it using the **Sentinel Module**

The work flow depicts the incoming traffic on a website this traffic is distinguished by understanding and analyzing the user behavior i.e if the user tries to ping in with an ip using port 80 or 443 i.e http to https it is directed to client website hosted by vm_80 where as if the user id trying to ping in using an ip on port 22 or 3389 i.e SSH or Rdp it is directed towards vm_rdp which servers as a honeypot.This differentiation in network is established using load balancer.

Once a failed rdp is done on vm_rdp it is logged in the security events of the windows OS this information is extracted and sent to a third party from which precise geolocation of the attackers is obtained and stored in a raw format in the vm.

A sample of this raw data is sent to administrators to train the log analytics beforehand.On competition of training the machine learning module in log analytics the raw data is sent in and are then further differentiated into custom logo and custom fields.

These custom fields are sent to sentinel to parse out the data in a graphical manner and represented to the client for better understanding.