LOCAL VM SETUP

VPC

Windows Server
RDP Enabled

Fleet Server

Ubuntu Server
SSH Enabled

Managed

Managed

Forward Logs via Agent

Manage Agents

Forward Logs via Agent

Private Network: 172.31.0.0/24
IP Range: 172.31.0.1-254
Subnet Mask: 255.255.255.0

Elastic & Kibana

Alerts/Tickets

OS Ticket Server

C2 Server
Mythic

Internet

Connect to Elastic/Kibana via Web GUI

SOC Analyst Laptop

Attacker Laptop
Kali Linux