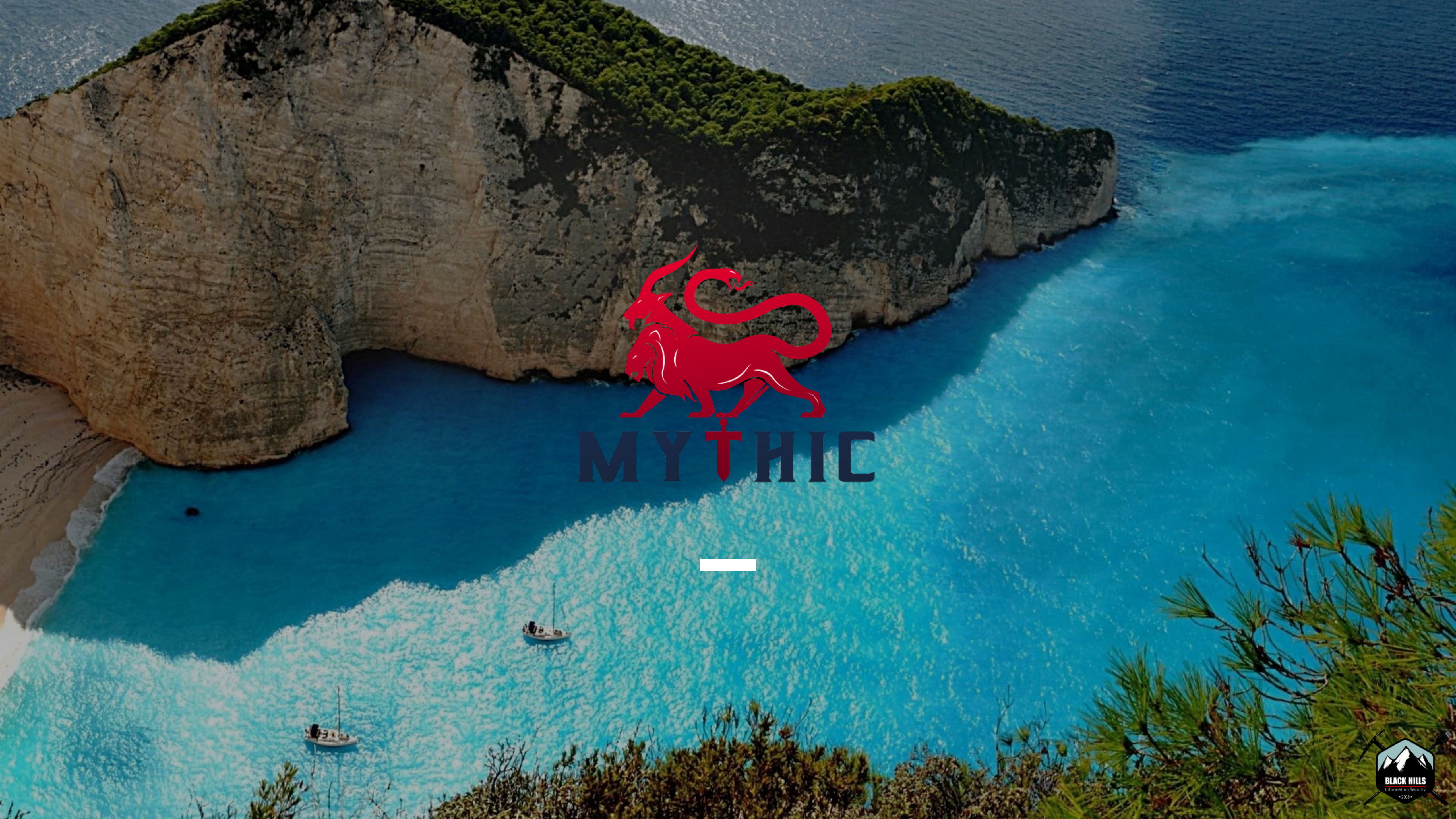




DevOps

FOR HACKERS
BY RALPH MAY



MYTHIC



Why Mythic

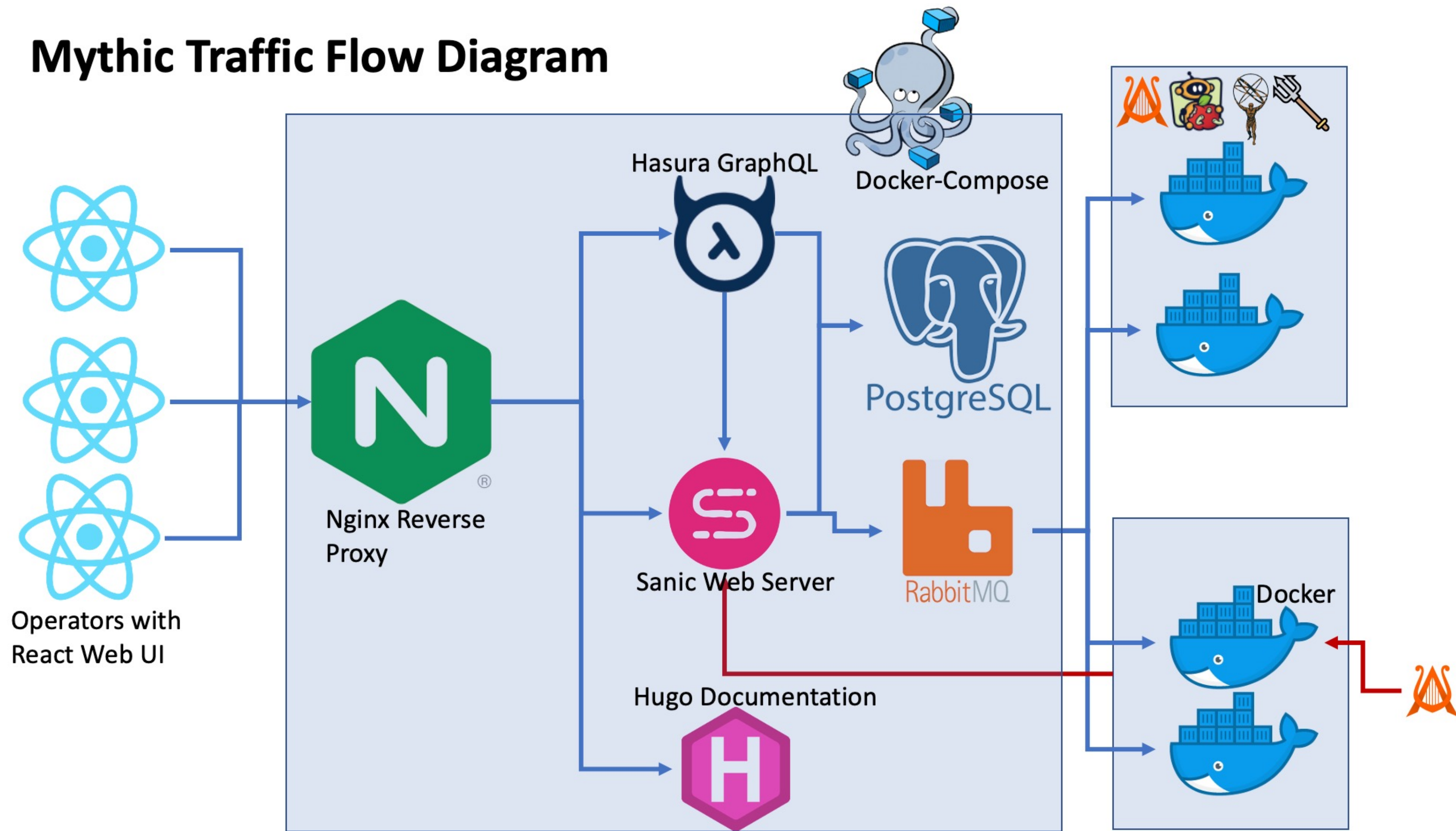
- Free / Open Source
- Docker - Baby
- Web interface / Multiple Users
- Bring Your Own Agent
- Build your own Opsec
- Not just for Windows

Mythic Pitfalls

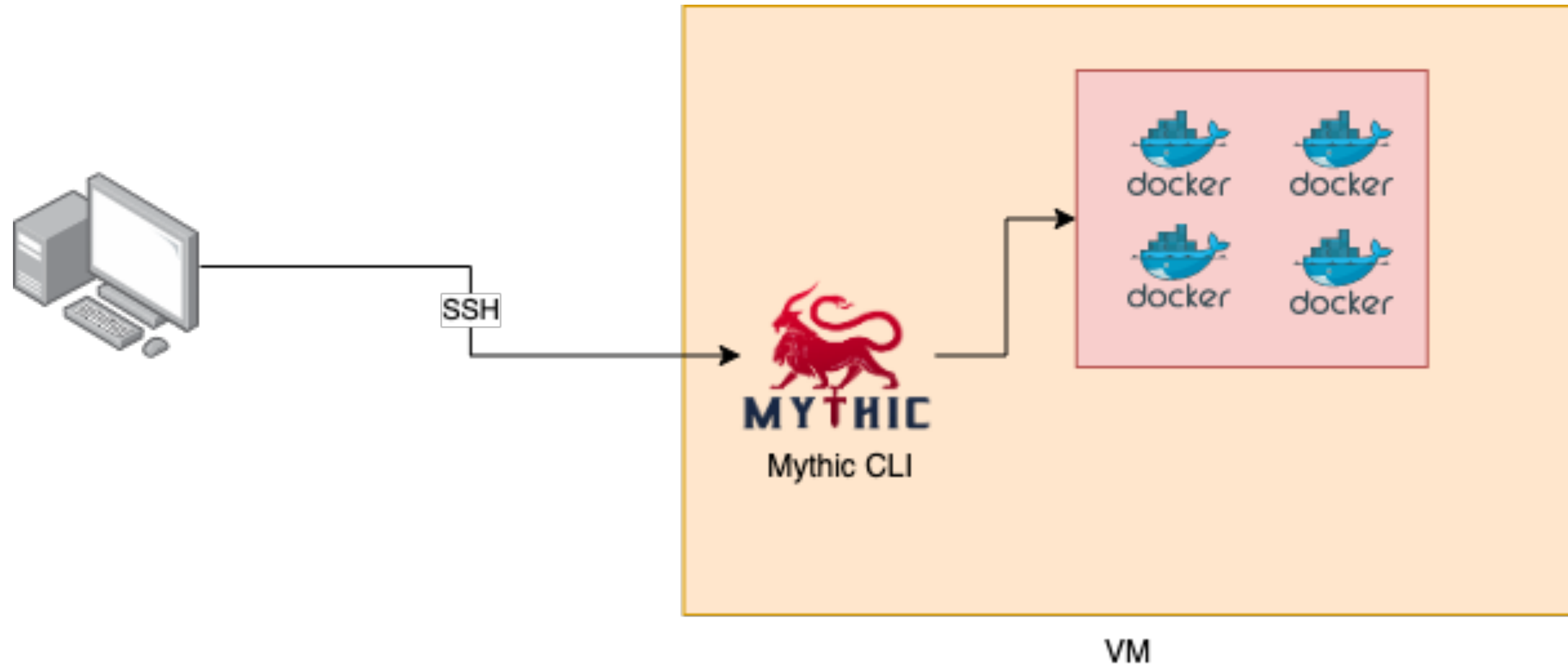
- You need to write your own agent.
- Reporting is limited
- Lots of Docker
- Not the simplest C2

Mythic Diagram

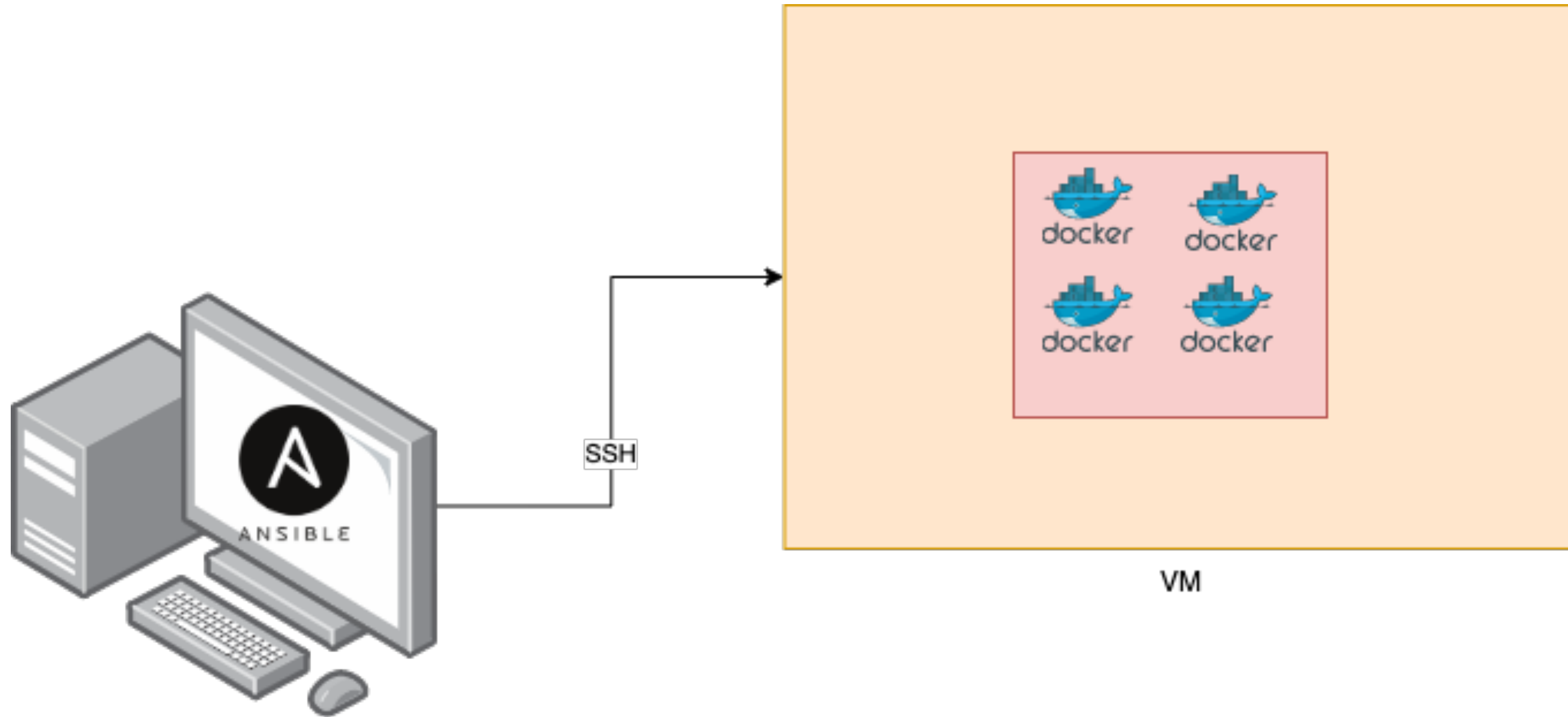
Mythic Traffic Flow Diagram



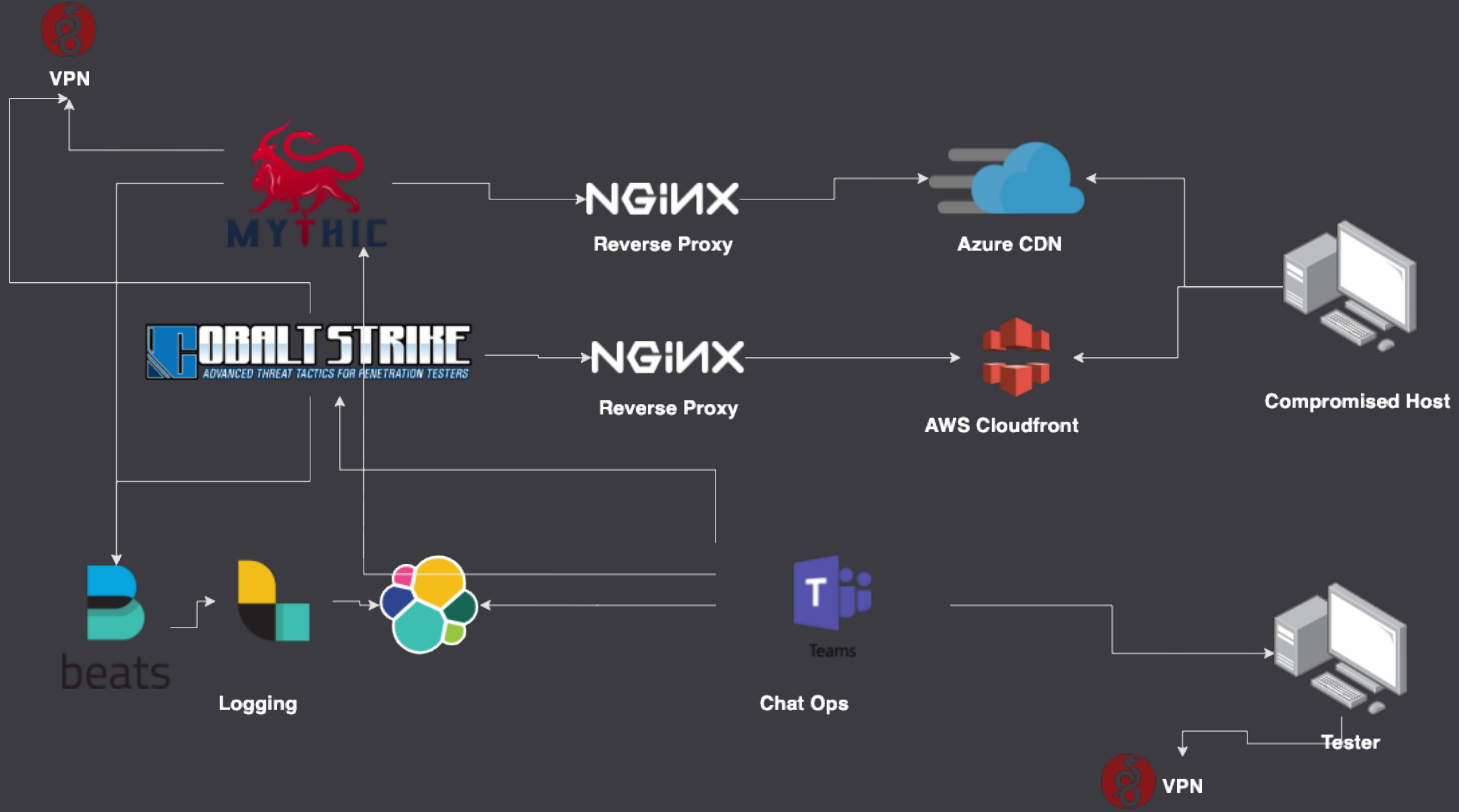
Standard Mythic Deployment



Ansible Mythic Deployment



Advanced Ansible Deployment



Version 2.2 >

Mythic

Operators

Installation v

Connecting

A note about containers

Updating Mythic

Internal Documentation

Quick Usage

Operational Pieces v

MITRE ATT&CK

Operations

Analytics

Browser Scripts

Act C&W Backs

Files

Tools

File Browser

Socks Proxy

Installation

Get the code

Pull the code from the official GitHub repository:

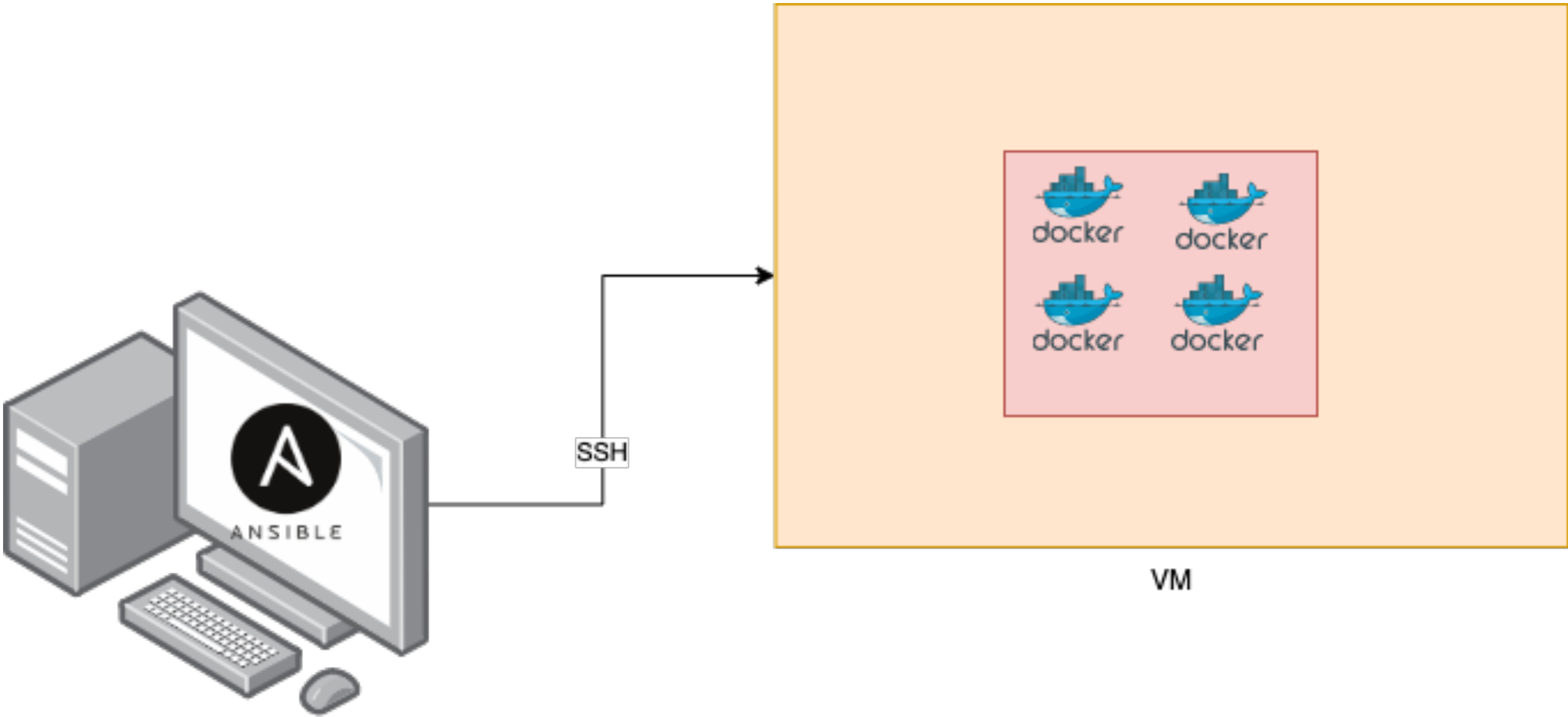
```
$ git clone https://github.com/its-a-feature/Mythic
```

i This is made to work with docker and docker-compose, so they both need to be installed. If docker is not installed on your ubuntu machine, you can use the `./install_docker_ubuntu.sh` script to install it for you. If you're running on debian, use the `./install_docker_debian.sh` instead.

STANDARD MYTHIC DEPLOYMENT (DEMO)

! Mythic must be installed on Linux. While macOS supports Docker and Docker-Compose, macOS doesn't handle the same networking that Mythic relies on. You can still access the Browser interface on macOS but the Mythic instance must be installed on Linux

Lab Overview



Lab 4

GOALS

Deploy the Mythic C2 Framework with Ansible.

- Build and add the Mythic C2 role
- Use Ansible to deploy Mythic C2 Server.
- Use Mythic to create a Windows Payload and run remote commands.

<https://workshop.hackerops.dev>

What's Next

HackerOps - 16 Hour Class

What to expect.

- Advanced Terraform Usage
- Advanced Ansible Usage
- Combining Ansible & Terraform into one playbook
- More clouds AWS/Azure
- Automate Build Pipelines With Github/Azure

What's Next

HackerOps - 16 Hour Class

- Labs
 - Deploying Elastic EDR and auto testing of payloads
 - Full C2 deployment
 - Payload Build
 - Phishing
 - Windows Lab

Questions



@ralphte1 Ralph May

