DevOps

FOR HACKERS

BY **RALPH MAY**

C2

CALLIDUS

MERLIN

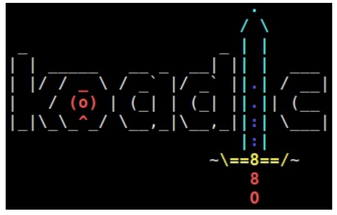
COVENANT

MYTHIC

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

PoshC2

SILENTTRINITY

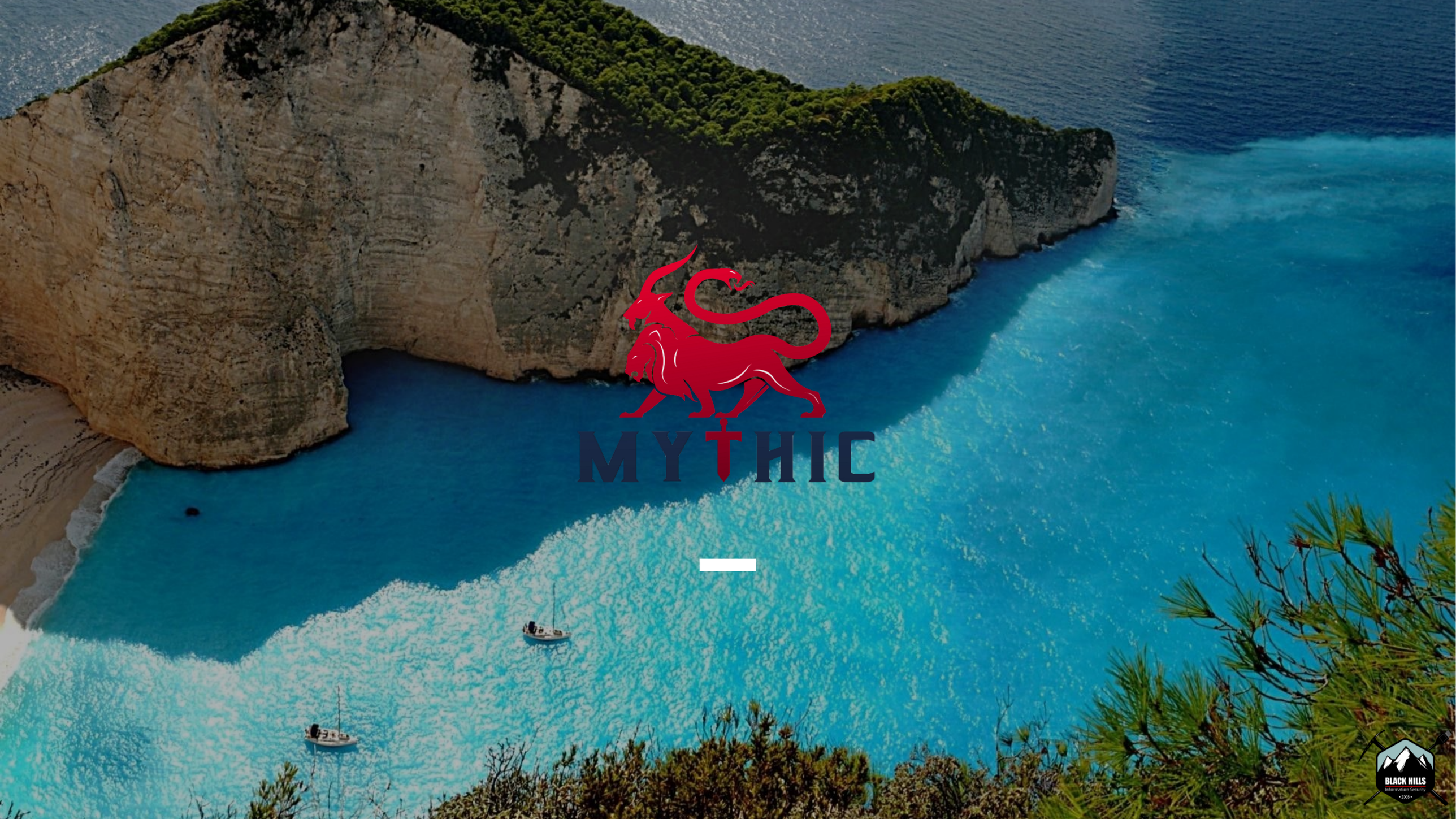


FACTION

CHAOS

Baby Shark

BLACK HILLS
Information Security


MYTHIC

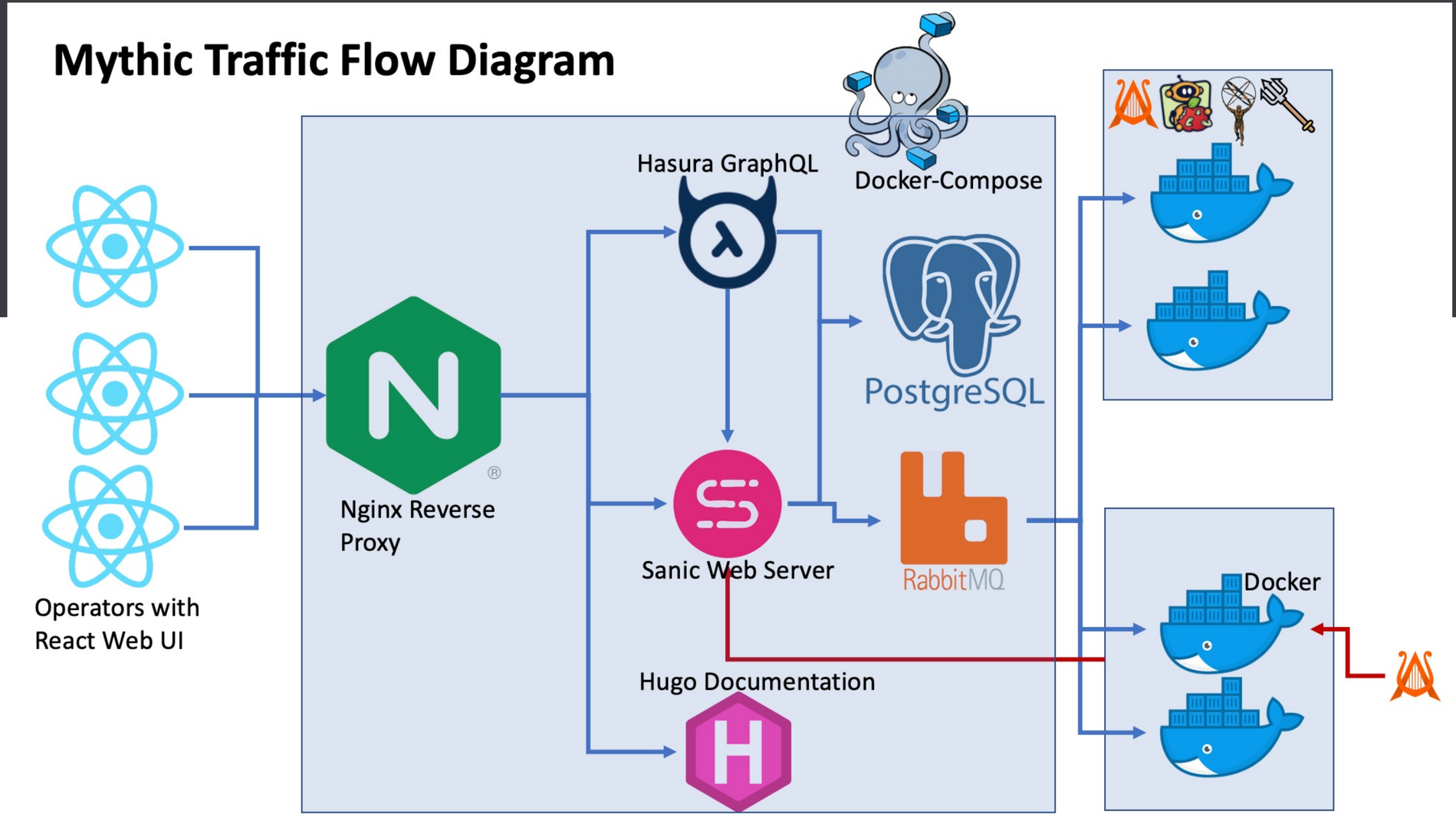
Why Mythic

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

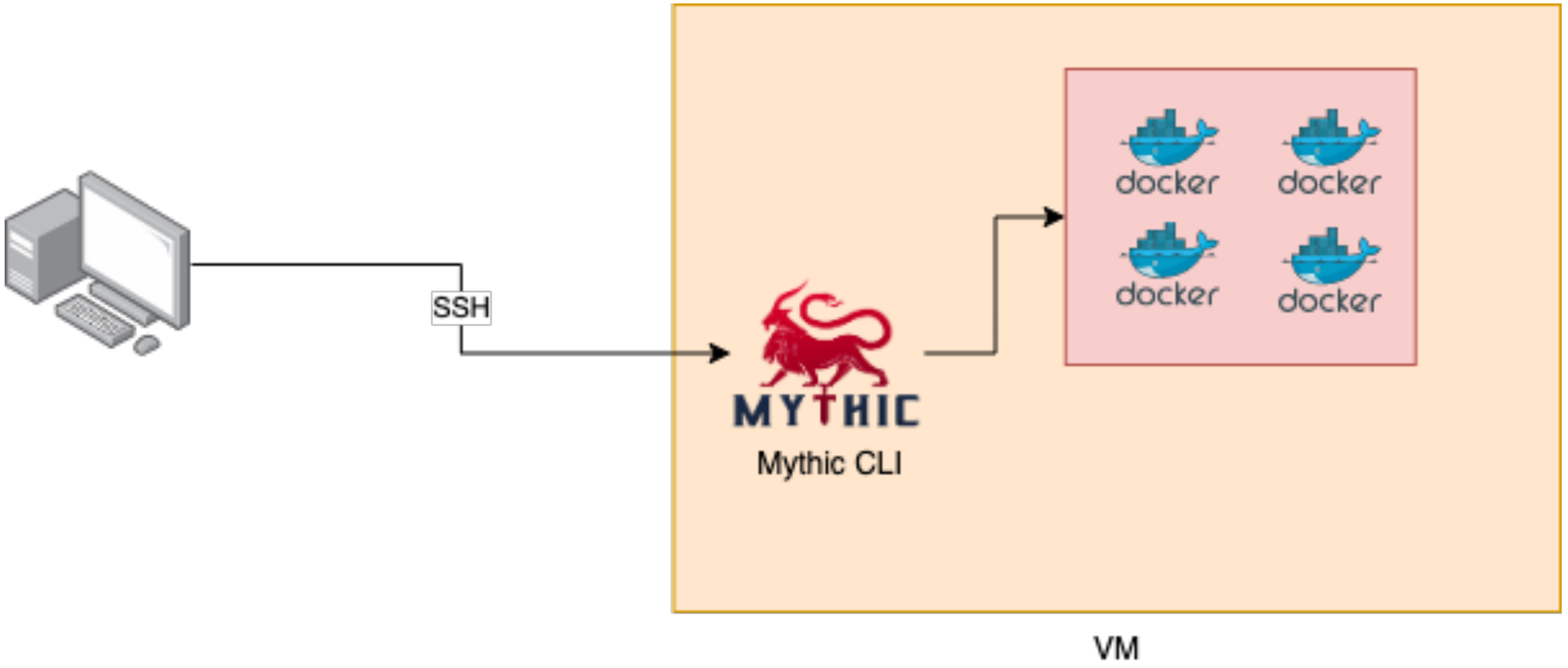
Mythic Pitfalls

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

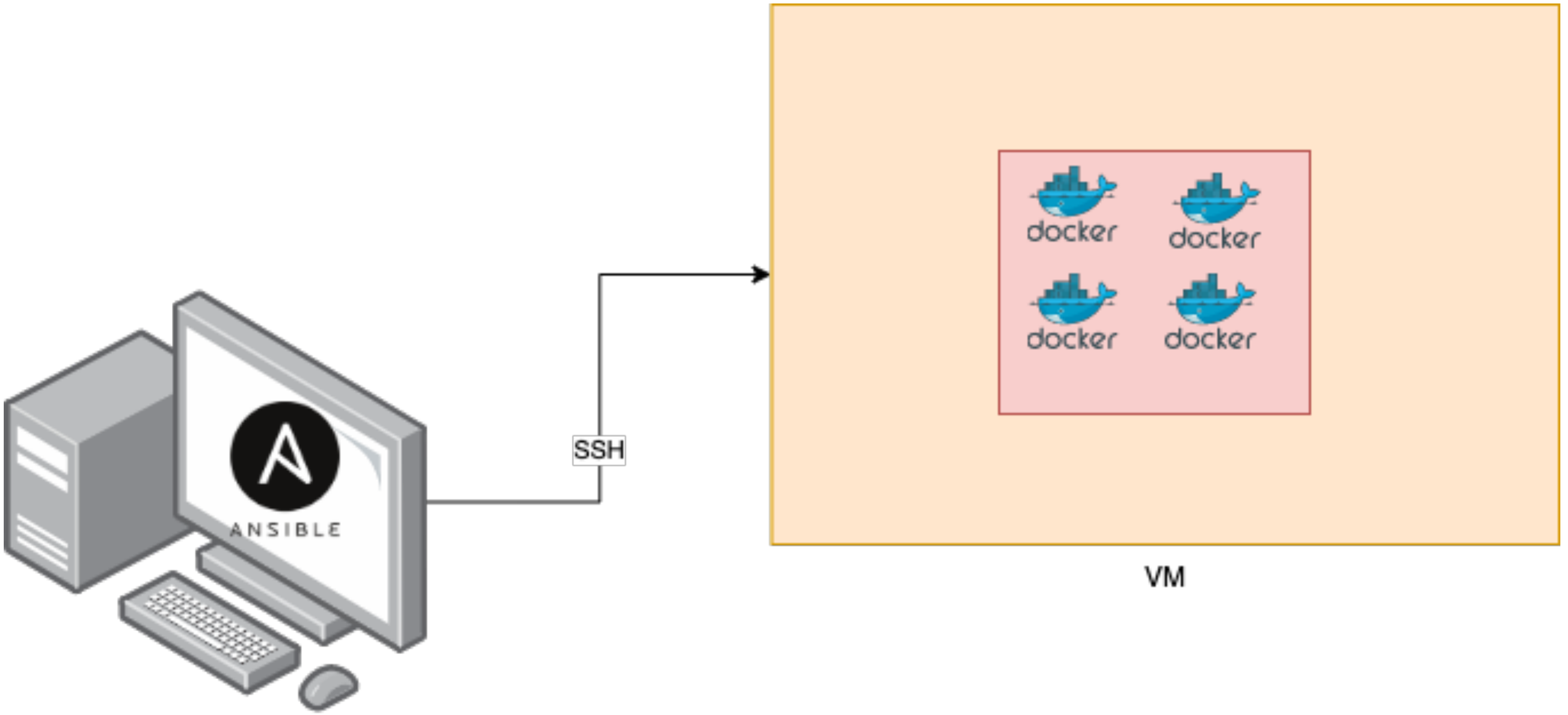
Mythic Diagram



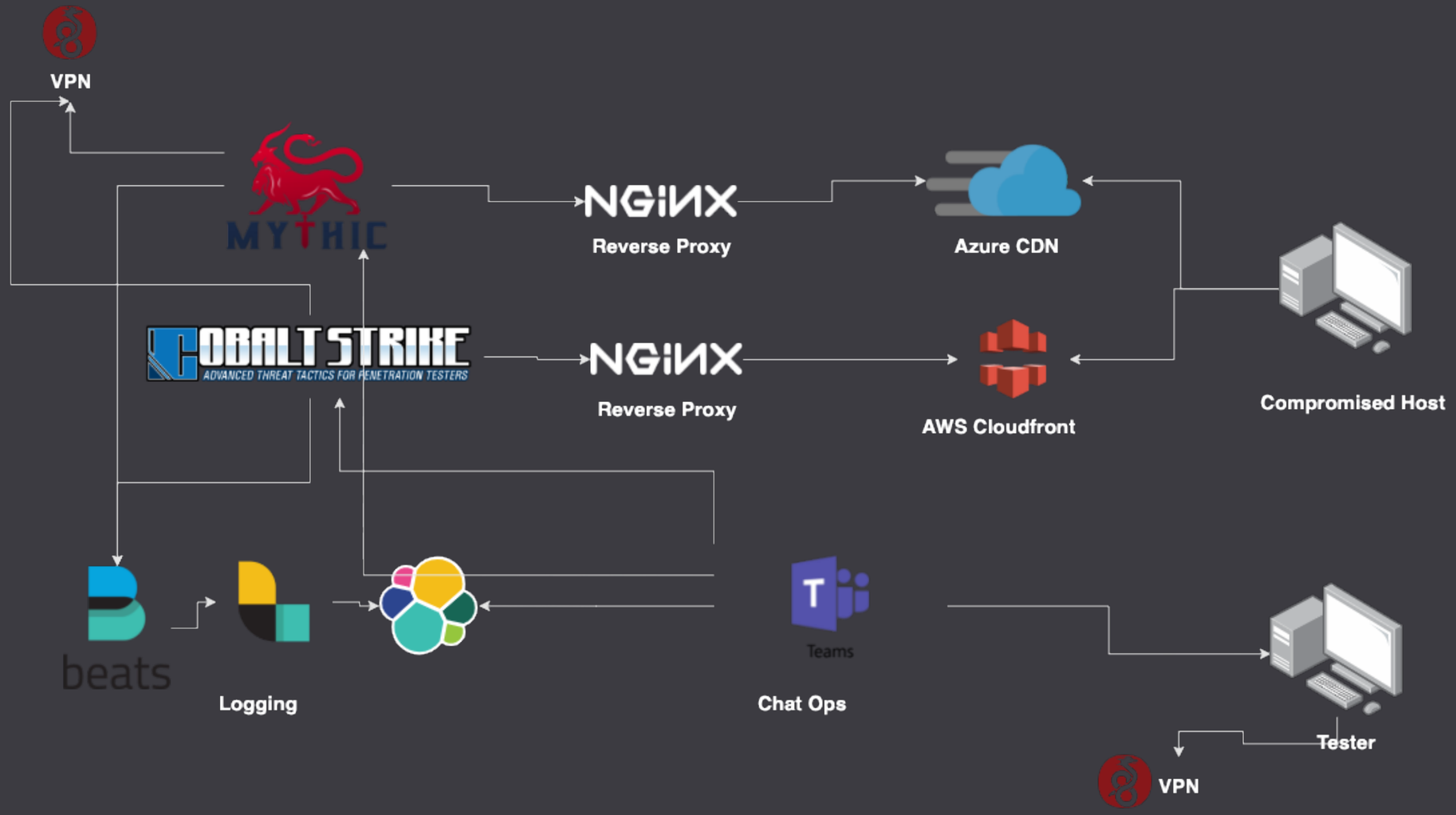
Standard Mythic Deployment

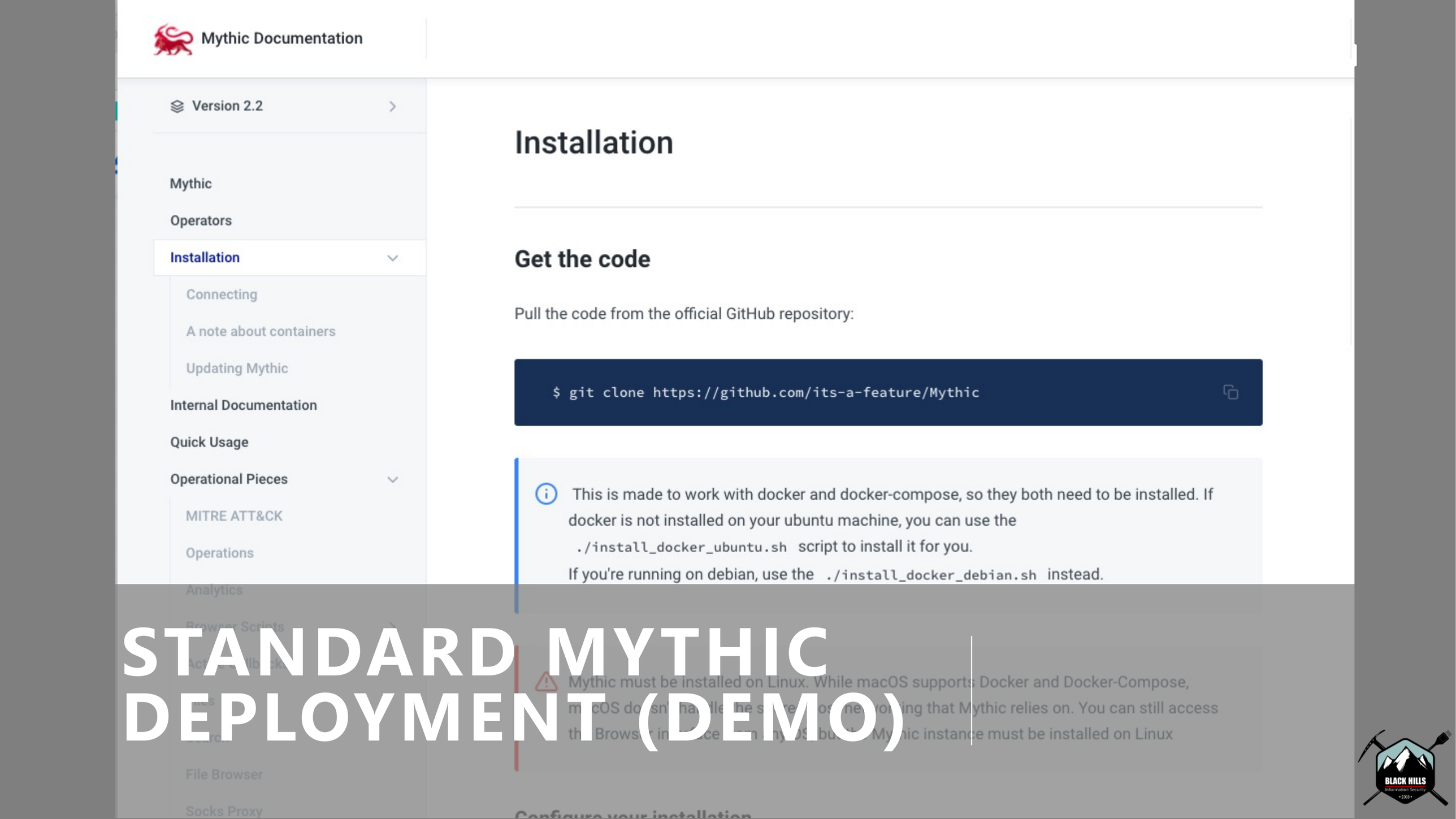


Ansible Mythic Deployment



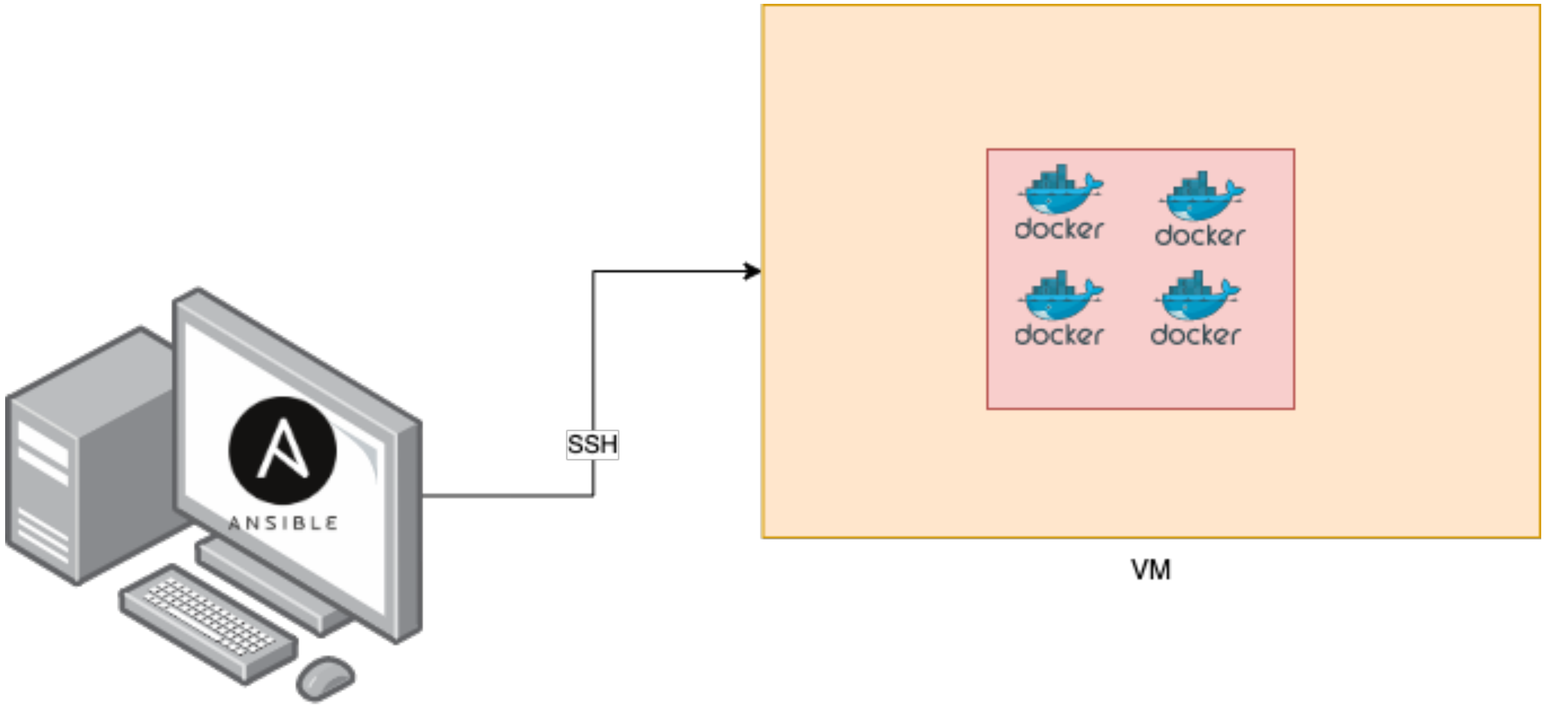
Advanced Ansible Deployment





STANDARD MYTHIC DEPLOYMENT (DEMO)

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

@ralphte1 Ralph May