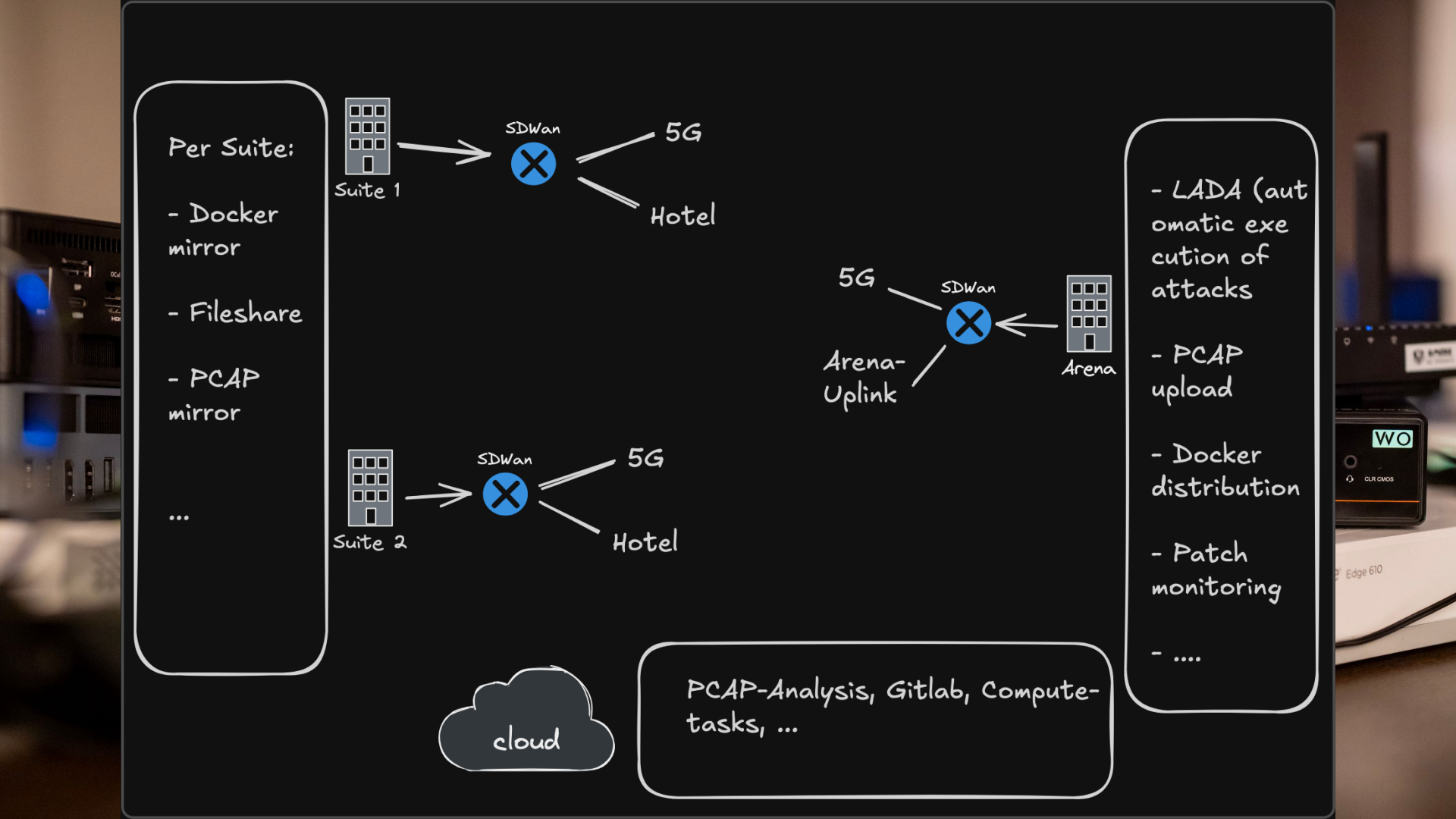

dynatrace
ERSTE SPARKASSE
TU WIEN
CYSEC
CYBERSECURITYCENTER
TU Graz
SBA Research
BOSCH
fh
st.pölten
JKU
JOHANNES KEPLER
UNIVERSITÄT LINZ
SIEMENS

Grandfather banned from US holiday after accidentally ticking 'terrorist' box on visa form

'I don’t know why that question is on the form in the first place'

WAITING FOR ALL THE ORGA TO BE DONE SO
I CAN FOCUS ON IMPORTANT STUFF (SHITPOSTING)


Per Suite:
- Docker mirror
- Fileshare
- PCAP mirror
...
Suite 1
SDWan
5G
Hotel
Suite 2
SDWan
5G
Hotel
5G
SDWan
Arena-Uplink
Arena
- LADA (automatic execution of attacks
- PCAP upload
- Docker distribution
- Patch monitoring
- ....
cloud
PCAP-Analysis, Gitlab, Compute-tasks, ...

Per Suite:

- Docker mirror
- Fileshare
- PCAP mirror

...

Suite 1 → SDWan → 5G / Hotel

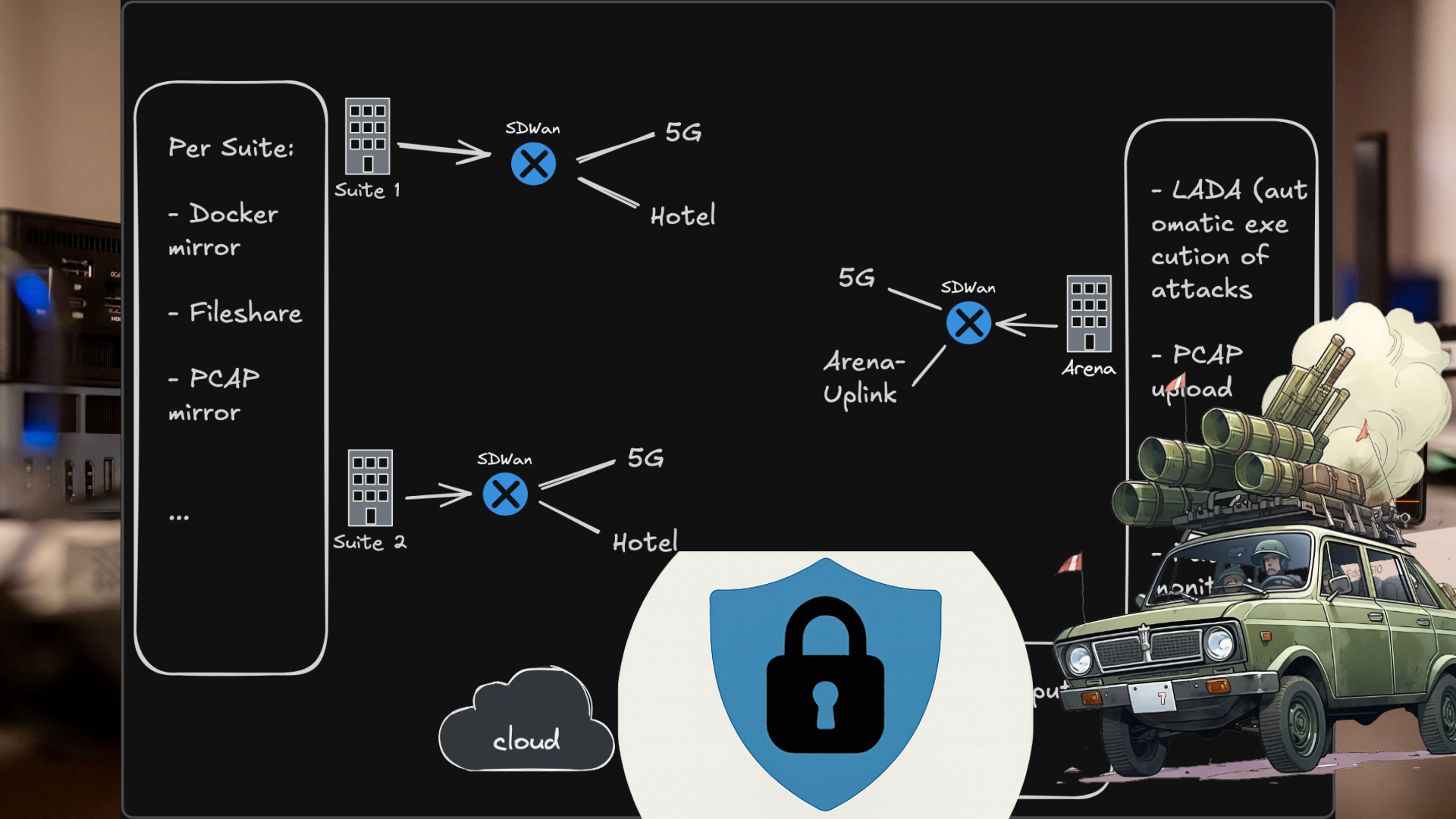
Suite 2 → SDWan → 5G / Hotel

5G / Arena-Uplink → SDWan → Arena

- LADA (automatic execution of attacks
- PCAP upload
- ...monit...

cloud

PCAP-Analysis, Gitlab, Compu... tasks, ...


Per Suite:
- Docker mirror
- Fileshare
- PCAP mirror
...
Suite 1
SDWan
5G
Hotel
Suite 2
SDWan
5G
Hotel
5G
SDWan
Arena-Uplink
Arena
- LADA (automatic execution of attacks
- PCAP upload
cloud

Per Suite:

- Docker mirror
- Fileshare
- PCAP mirror

Suite 1

SDWan

5G

Hotel

Suite 2

SDWan

5G

Hotel

5G

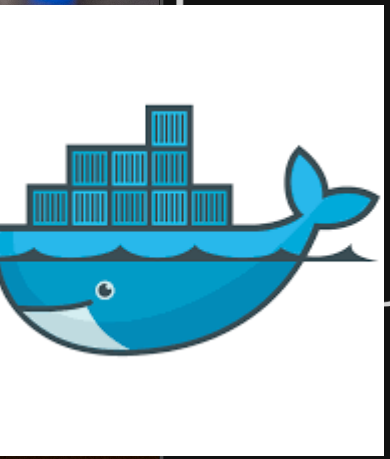
SDWan

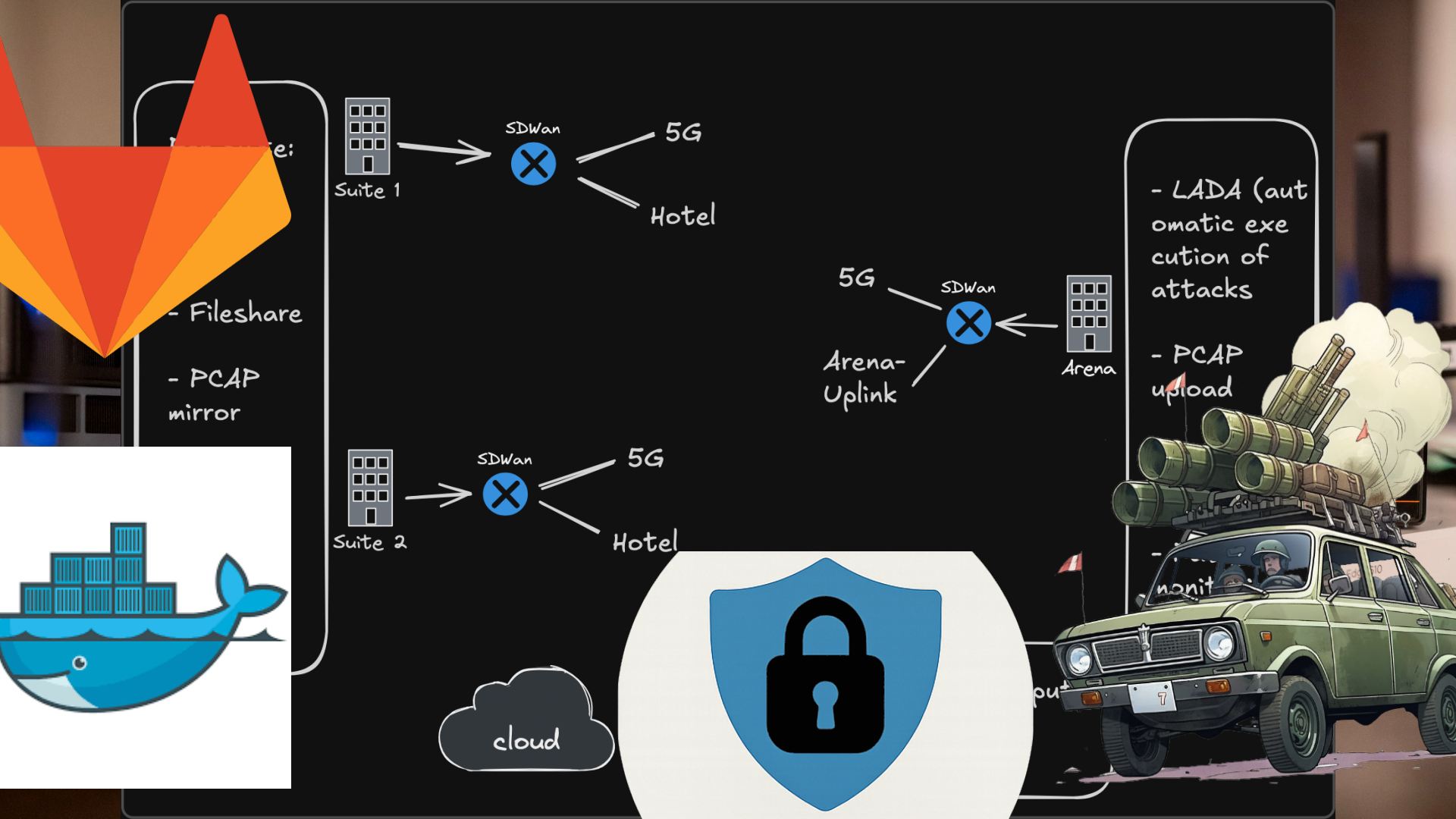
Arena-Uplink

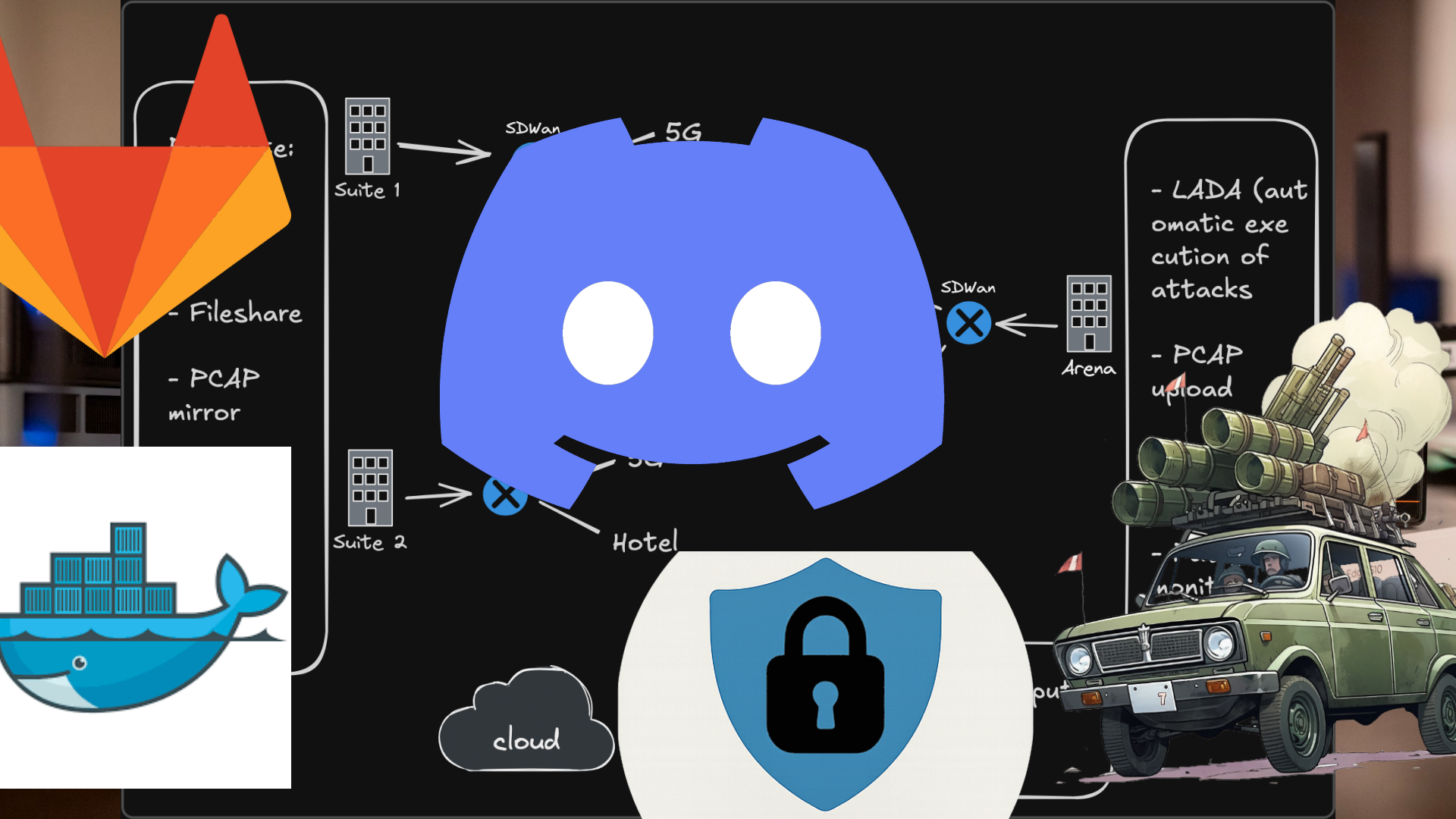
Arena

- LADA (automatic execution of attacks
- PCAP upload
- monit

cloud




- Fileshare
- PCAP mirror
Suite 1
SDWan
5G
Hotel
5G
SDWan
Arena-Uplink
Arena
- LADA (automatic execution of attacks
- PCAP upload
Suite 2
SDWan
5G
Hotel
cloud


- Fileshare
- PCAP mirror
Suite 1
SDWan
5G
SDWan
Arena
- LADA (automatic execution of attacks
- PCAP upload
Suite 2
Hotel
cloud

2x SDWAN Box Small
1x SDWAN Box Large
1x 5G Modem Netgear M6 Pro 5G WiFi 6E MR6450
1x UniFi UAP-AC-LR
1x Mini PC (Ryzen 7 7840HS 8 cores, 64GB RAM, 1TB SSD)
1x Mini PC
1x Mini PC (12 cores, 32GB RAM, 1TB SSD)
1x Mini PC (10 cores, 16GB Ram)
1x Laptop (i9-13900H, 64GB Ram)
1x 5G Router (huawei 5g cpe pro 2)
1x Netgear 5 Port Managed Switch
1x Netgear 5 Port UnManaged Switch
1x Netgear 16 Port Managed Switch

1x Unifi 24 Port Managed Switch (24x 1Gbit lan, 2x SFP+ 10G)
1x Unifi Outdoor AP (U6 Mesh Pro)
1x Netgear 8 Port Managed Switch
4x Power Strips, 6 sockets (with switches)
2x Power Strips, 6 sockets
1x Xiaomi AX5400 5G

We arrived!

– 69 Hours until game open –


dynatrace

- Setup A/D infra

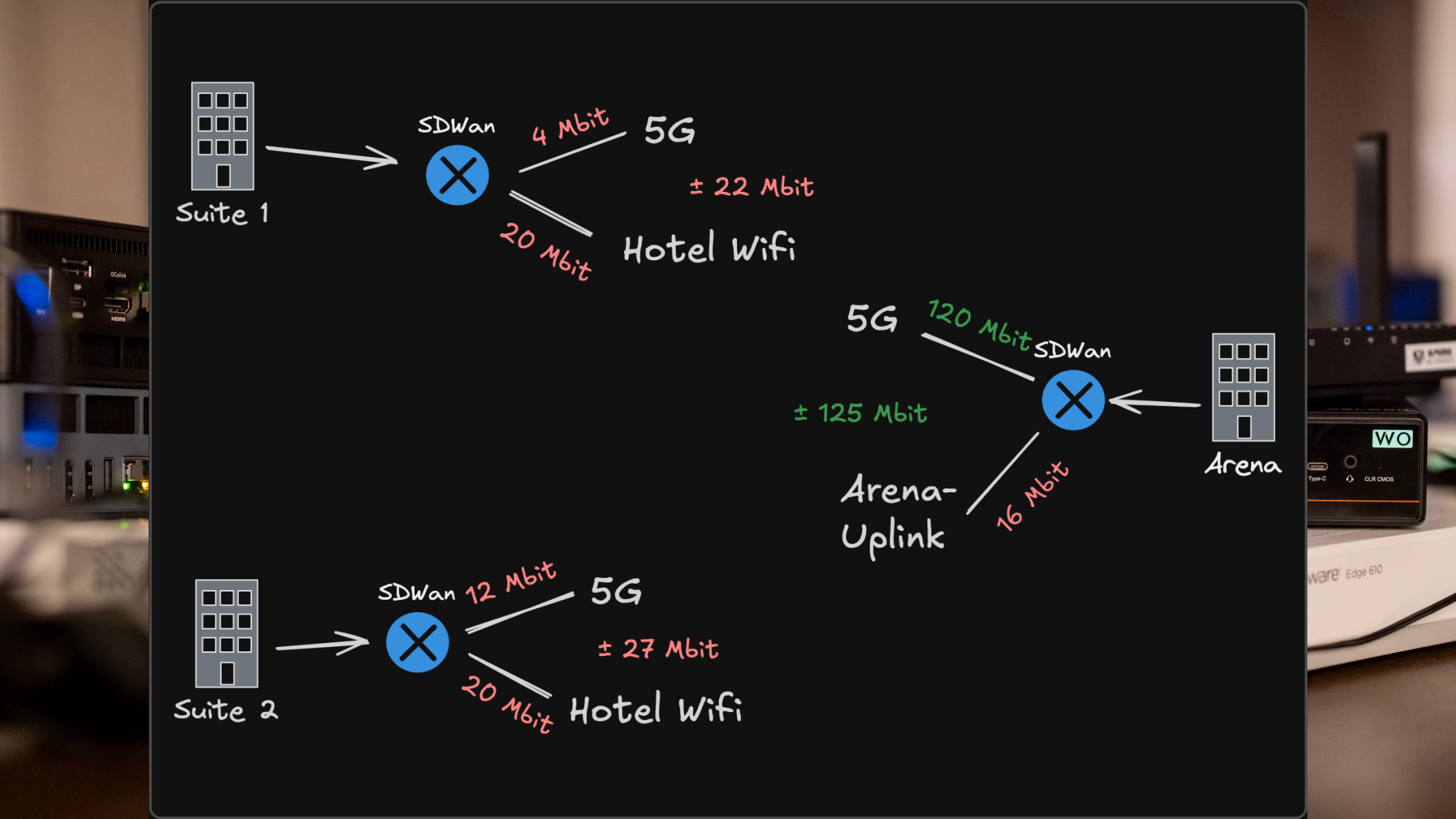
- Setup A/D infra
- Switched from Loki/Grafana to Dynatrace

- Setup A/D infra
- Switched from Loki/Grafana to Dynatrace

- Organize food and water

- Setup A/D infra
- Switched from Loki/Grafana to Dynatrace

- Organize food and water
- Buy 5G Routers


Suite 1
SDWan
4 Mbit
5G
± 22 Mbit
20 Mbit
Hotel Wifi
5G
120 Mbit
SDWan
± 125 Mbit
Arena
Arena-
Uplink
16 Mbit
Suite 2
SDWan
12 Mbit
5G
± 27 Mbit
20 Mbit
Hotel Wifi


MIDNIGHT SUN
CTF AND CONFERENCE

3

2

1


3
hours
sleep
2
1

3 hours sleep

2 proper meals

1

3 hours sleep

2 proper meals

1 shower

A/D

Services you have to find weaknesses to fix/attack

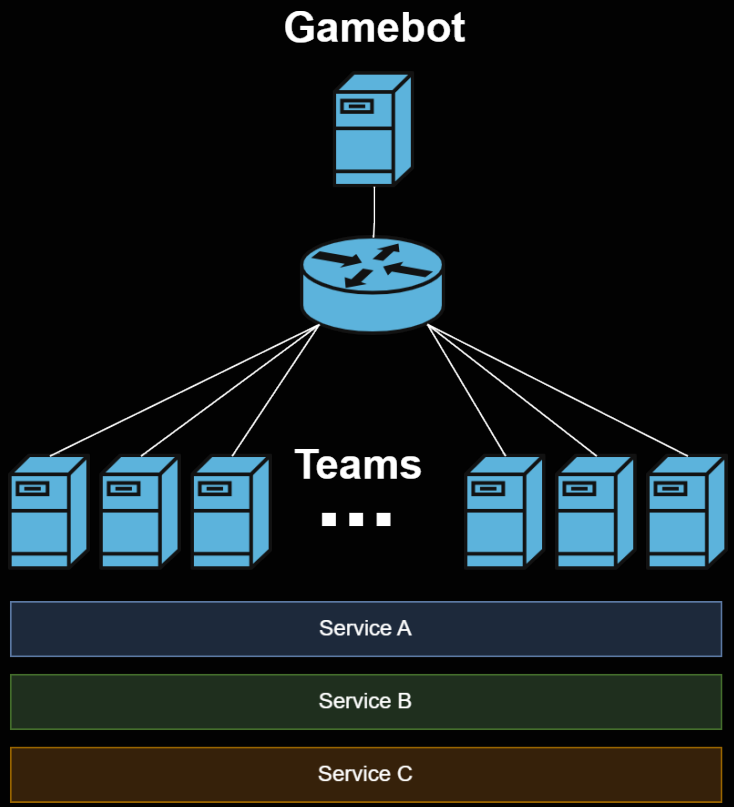
King of the Hill

Incremental challenges that give points according to rank

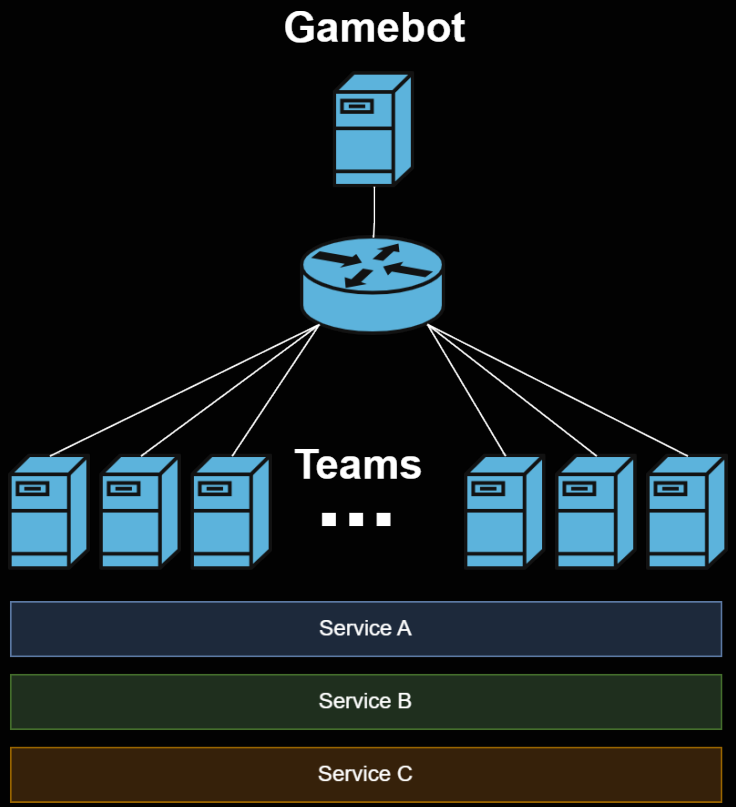
LiveCTF

Double elimination 1v1 tournament hacking on stage

How to A/D

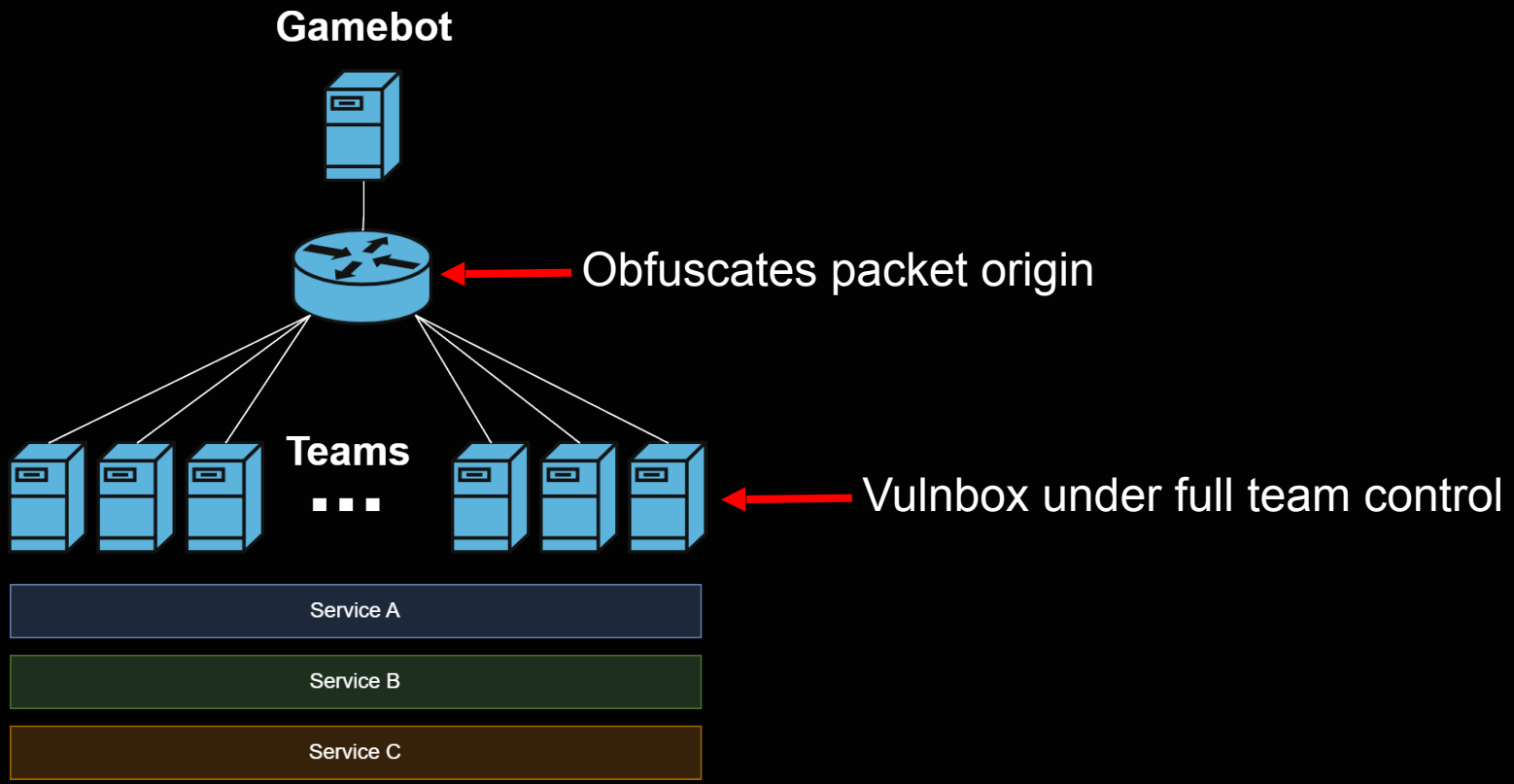


How to A/D

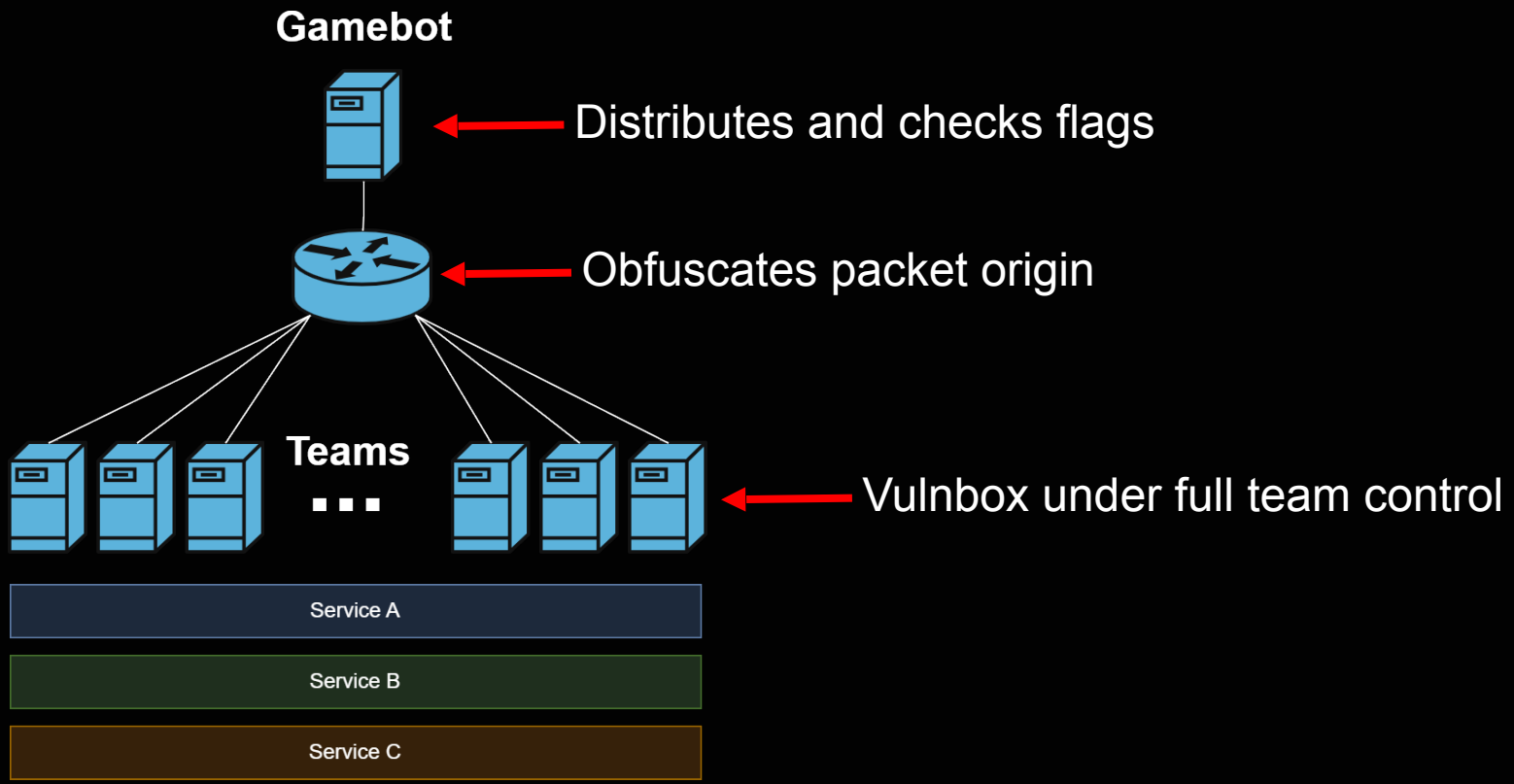


Vulnbox under full team control

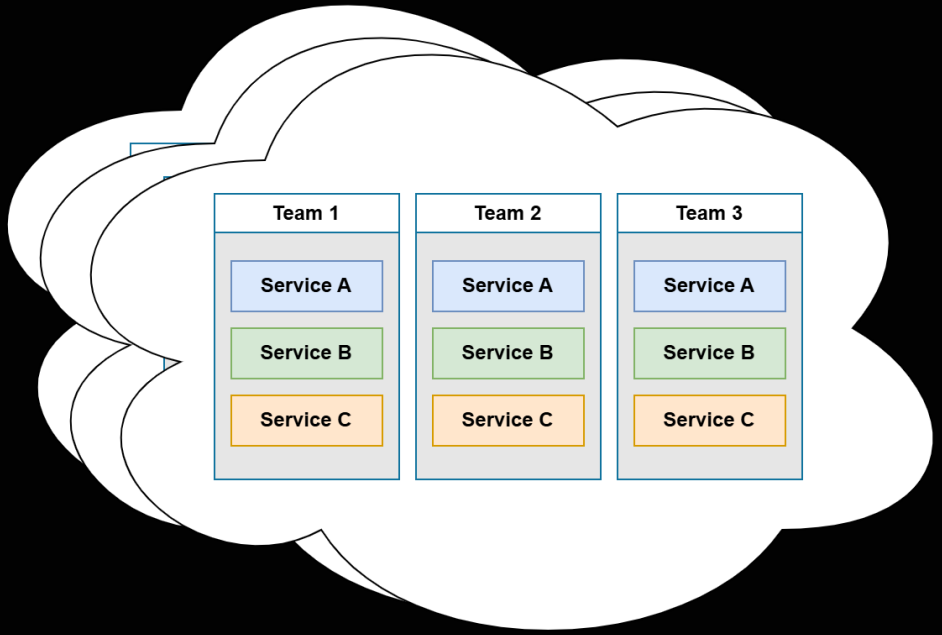
How to A/D


Gamebot
Obfuscates packet origin
Teams
Vulnbox under full team control
Service A
Service B
Service C

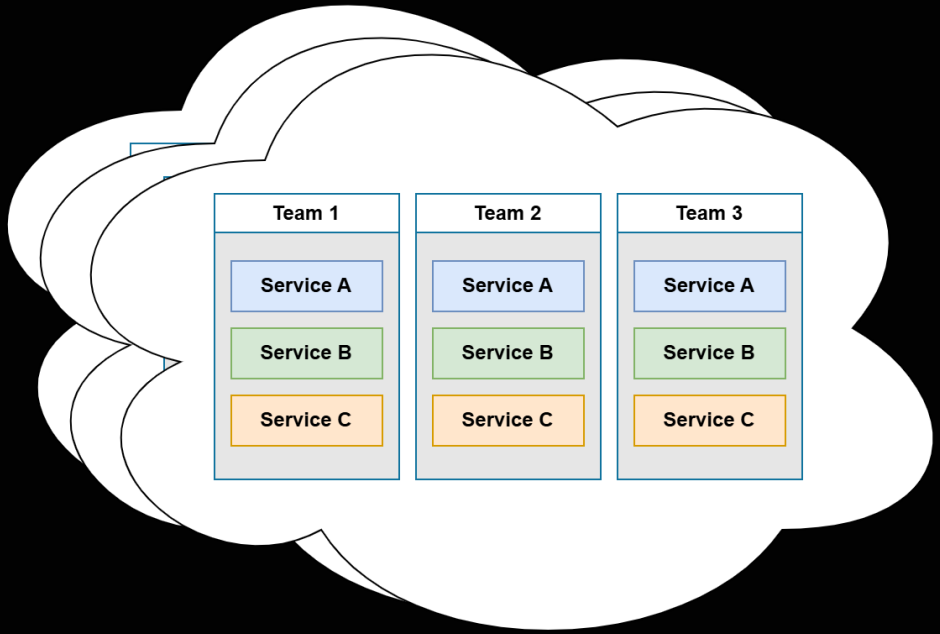
How to A/D


Gamebot
Distributes and checks flags
Obfuscates packet origin
Teams
Vulnbox under full team control
Service A
Service B
Service C

How to DEF CON A/D

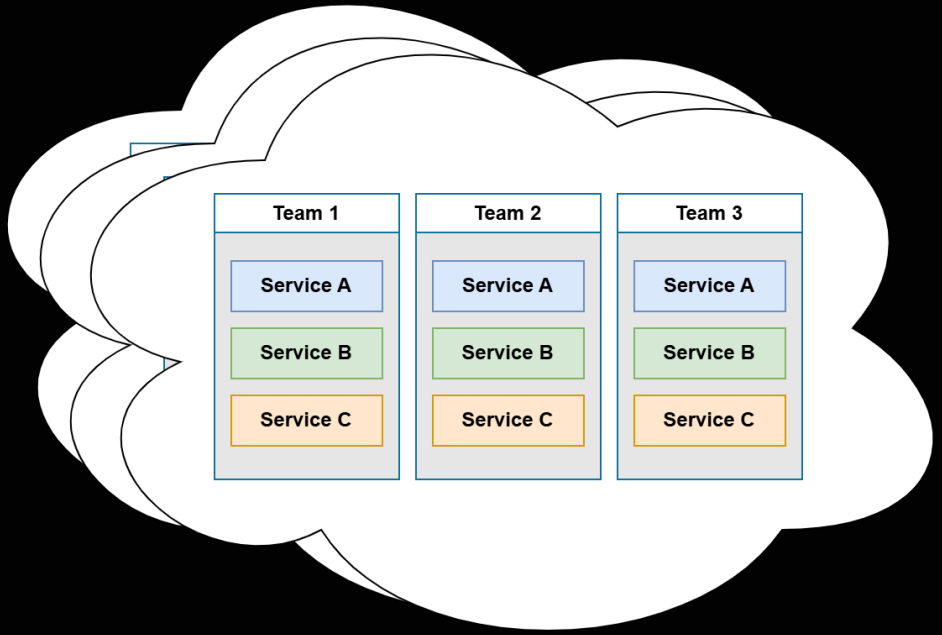


How to DEF CON A/D



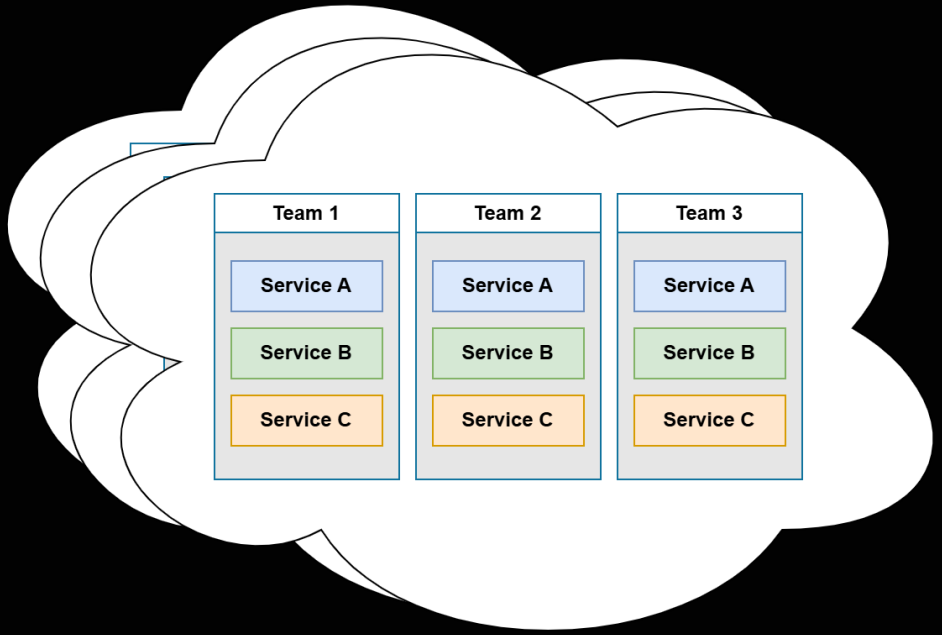
- Each service wrapped in docker

How to DEF CON A/D



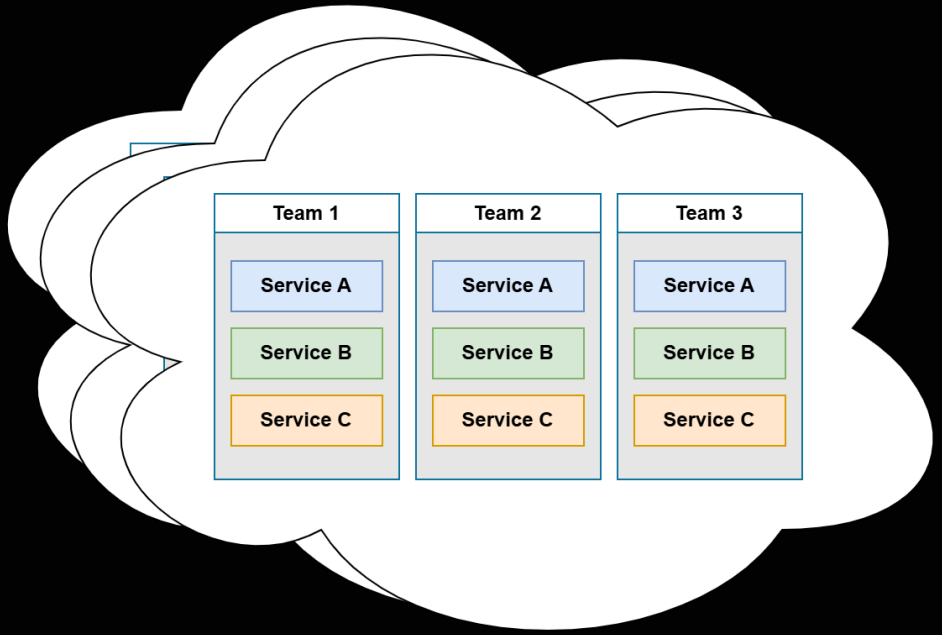
- Each service wrapped in docker
- Services hosted on organiser infra

How to DEF CON A/D



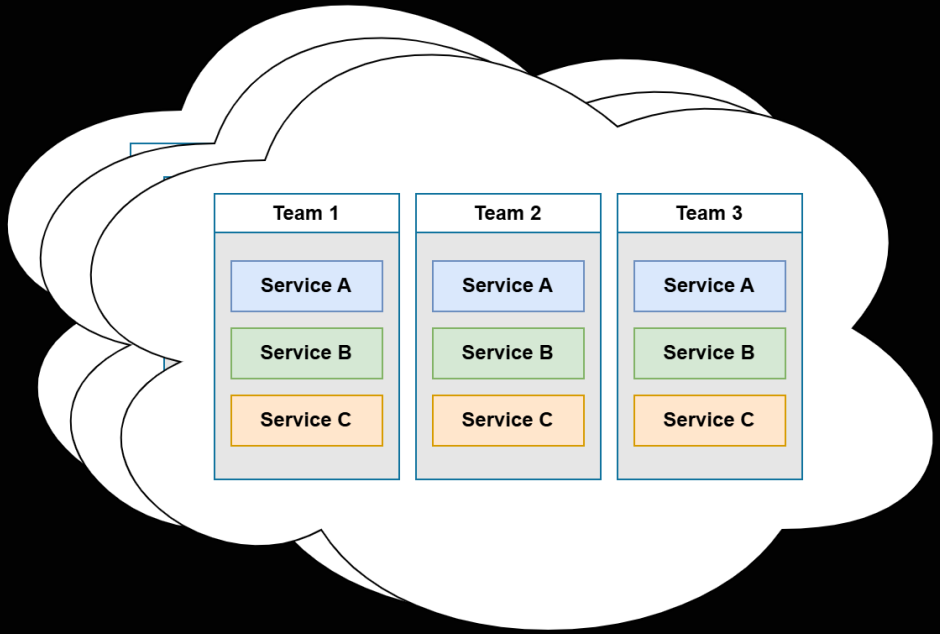
- Each service wrapped in docker
- Services hosted on organiser infra
- No. of containers:

How to DEF CON A/D



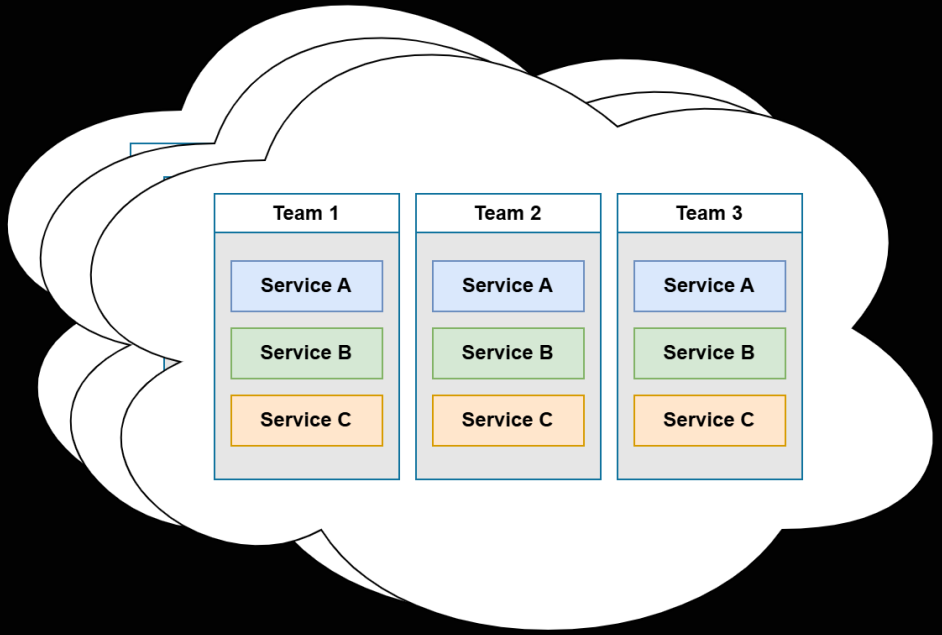
- Each service wrapped in docker
- Services hosted on organiser infra
- No. of containers:
  - Team X Team X services ~ 1200

How to DEF CON A/D



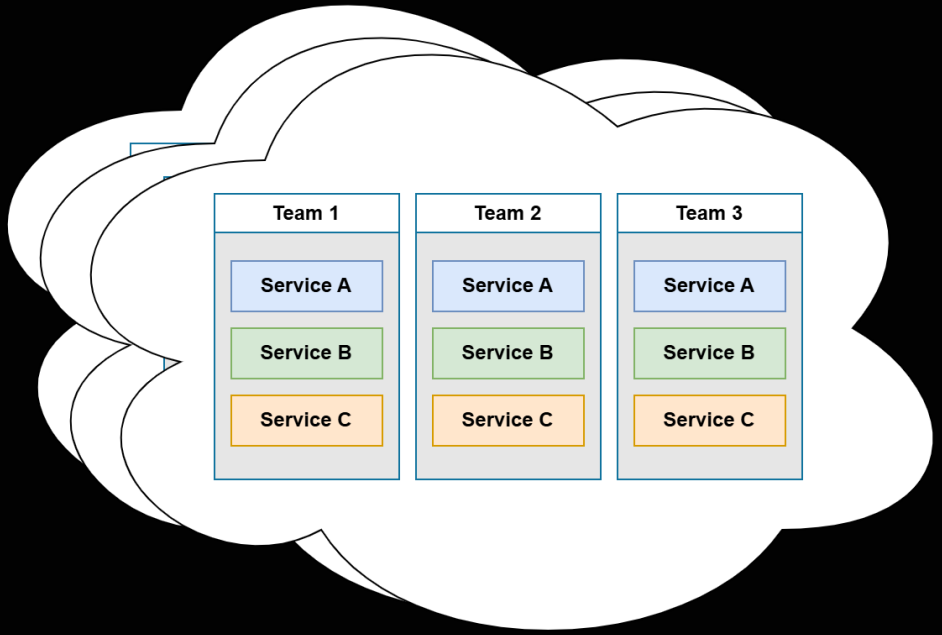
- Each service wrapped in docker
- Services hosted on organiser infra
- No. of containers:
  - Team X Team X services ~ 1200
- Attack box still under team control

How to DEF CON A/D



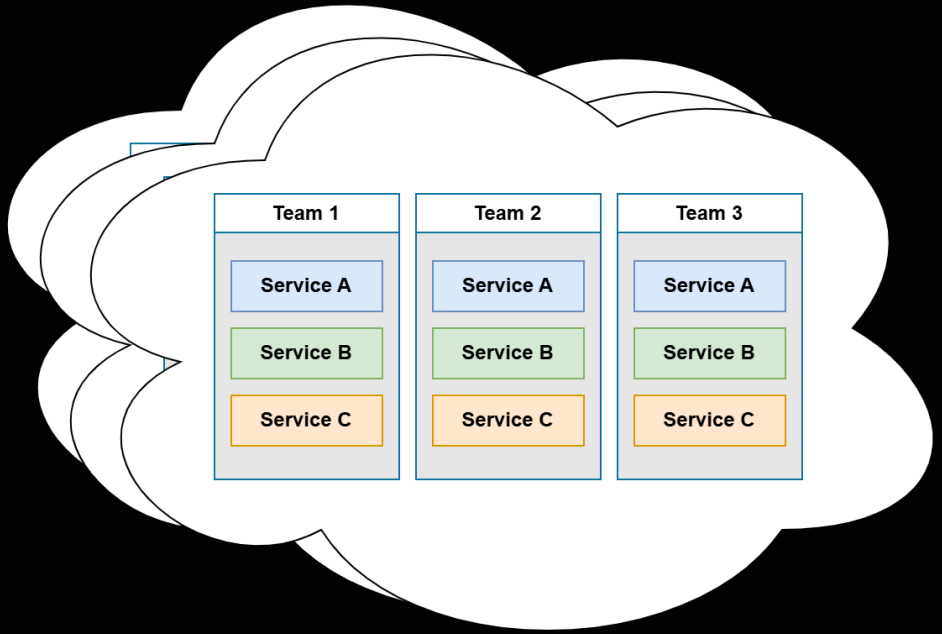
- Each service wrapped in docker
- Services hosted on organiser infra
- No. of containers:
  - Team X Team X services ~ 1200
- Attack box still under team control
- Attacks in silent mode (no traces) - but less points

How to DEF CON A/D



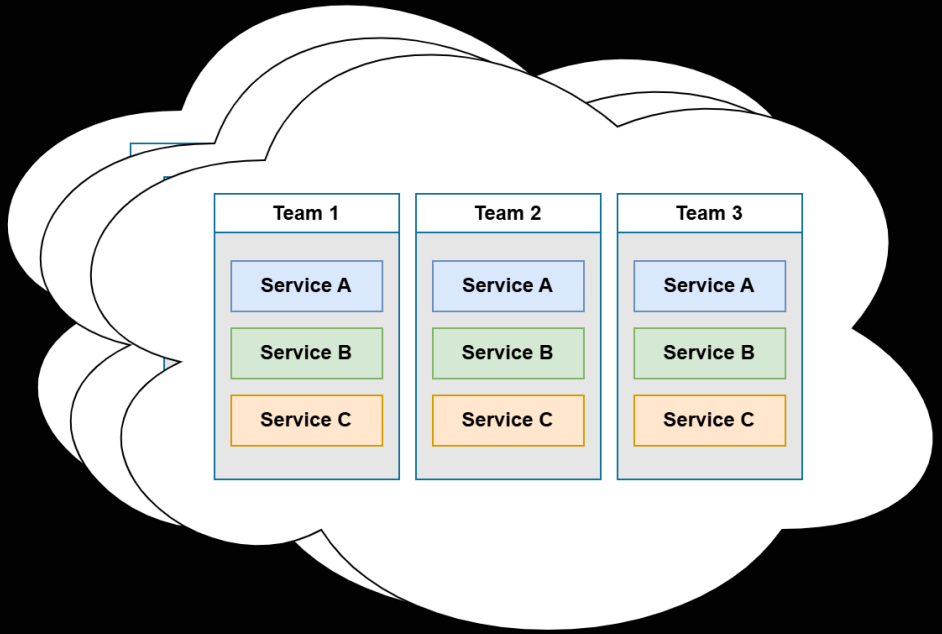
- Each service wrapped in docker
- Services hosted on organiser infra
- No. of containers:
  - Team X Team X services ~ 1200
- Attack box still under team control
- Attacks in silent mode (no traces) - but less points
- Patches are public

How to DEF CON A/D



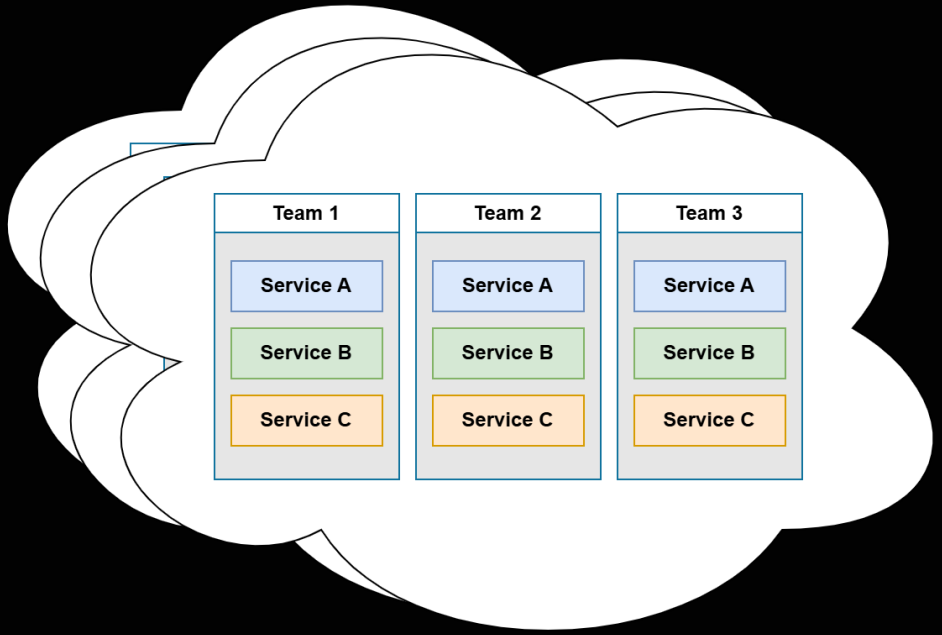
- Each service wrapped in docker
- Services hosted on organiser infra
- No. of containers:
  - Team X Team X services ~ 1200
- Attack box still under team control
- Attacks in silent mode (no traces) - but less points
- Patches are public
- Network traces are public

How to DEF CON A/D



- Each service wrapped in docker
- Services hosted on organiser infra
- No. of containers:
  - Team X Team X services ~ 1200
- Attack box still under team control
- Attacks in silent mode (no traces) - but less points
- Patches are public
- Network traces are public
- Each team gets dedicated infra

How to DEF CON A/D



- Each service wrapped in docker
- Services hosted on organiser infra
- No. of containers:
  - Team X Team X services ~ 1200
- Attack box still under team control
- Attacks in silent mode (no traces) - but less points
- Patches are public
- Network traces are public
- Each team gets dedicated infra
  - -> no interference