


# From lonely wolf to the pack

Cyber playground evolution

# /whoami

- Sebastian PITEI (@sebypp) 
- Infra & Security @Bit Sentinel
- networking, infrastructure, security, programming (but only the fun stuff)

# First CTF?

1993 @DEFCON



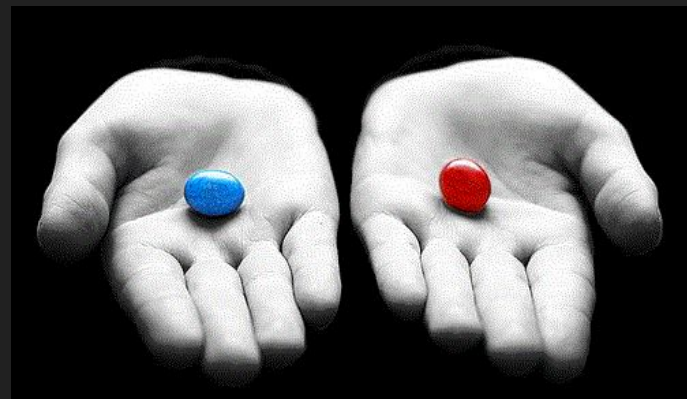
# CTF

- lone wolf
- you get to learn *some* things
- *sometimes* it's not *that* close to real life
- it's fun
- it lasts as long as you want
- can add bias toward Red
- probably not enough Blue
- it's somewhat easier to organise



# Attack & Defence

- part of the pack
- broader skill set (not complete, though)
- closer-*ish* to real life scenarios
- it's still fun!
- time is of the essence
- balanced Blue/Red approach
- extremely time consuming to organize



[insert name here...]

- “The Times They Are a-Changin”
- Simple Attack & Defence
- Plugable chall system
- One-click operation (for both players & game-masters) with low deployment time
- Minimum reqs (bear minimum, you’ll need a computer with a browser)
- Highly scalable!

# Automation

- interact with the infrastructure environment
- full IaC for all relevant parts of the system (challs, VPN, scoring server)
- self-deployable, no reliance on 3rd party “tools”
- nice to have: API!



**RED HAT**<sup>®</sup>  
**ANSIBLE**<sup>®</sup>

# Infrastructure

- readily available
- deployable in public and private cloud
- has large support for other “goodies” than virtual machines

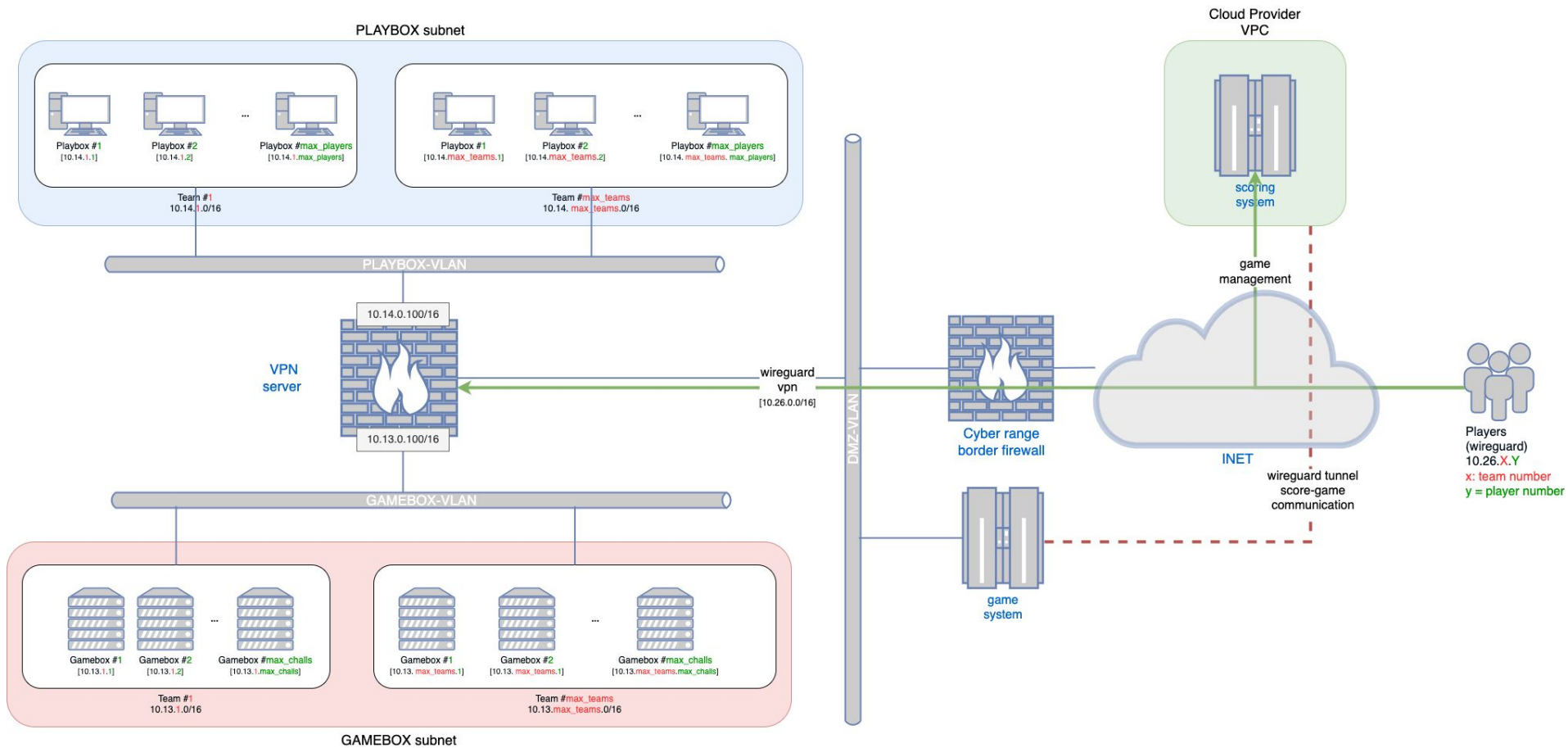


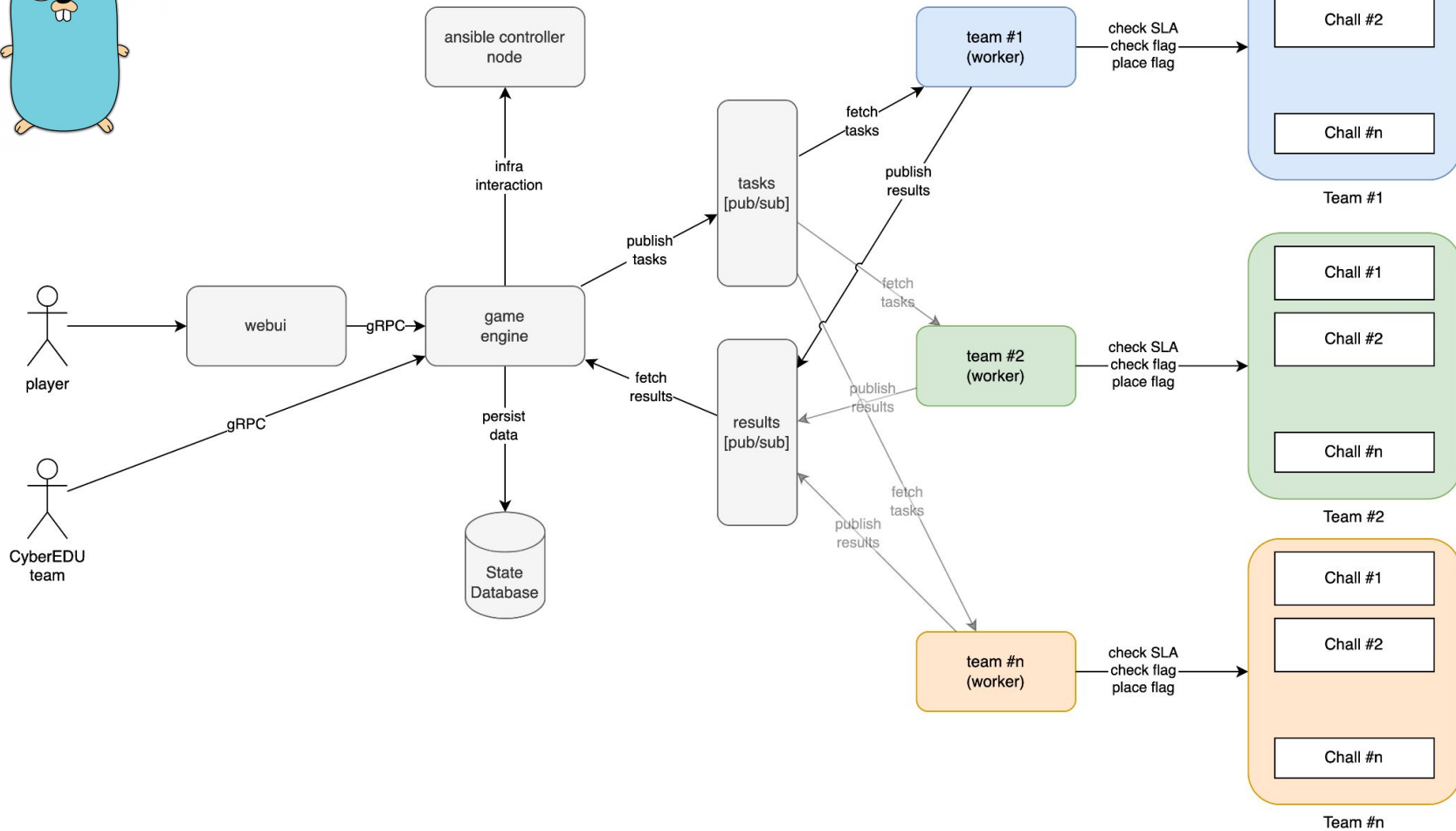
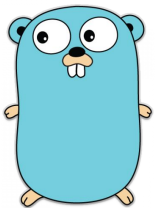
# Challs (i.e. gameboxes)

- simulate real life (“upgrade” from containers to VMs)
- decouple development from deployment

# Players (i.e. playboxes)

- have all the tools readily available
- fast and easy access

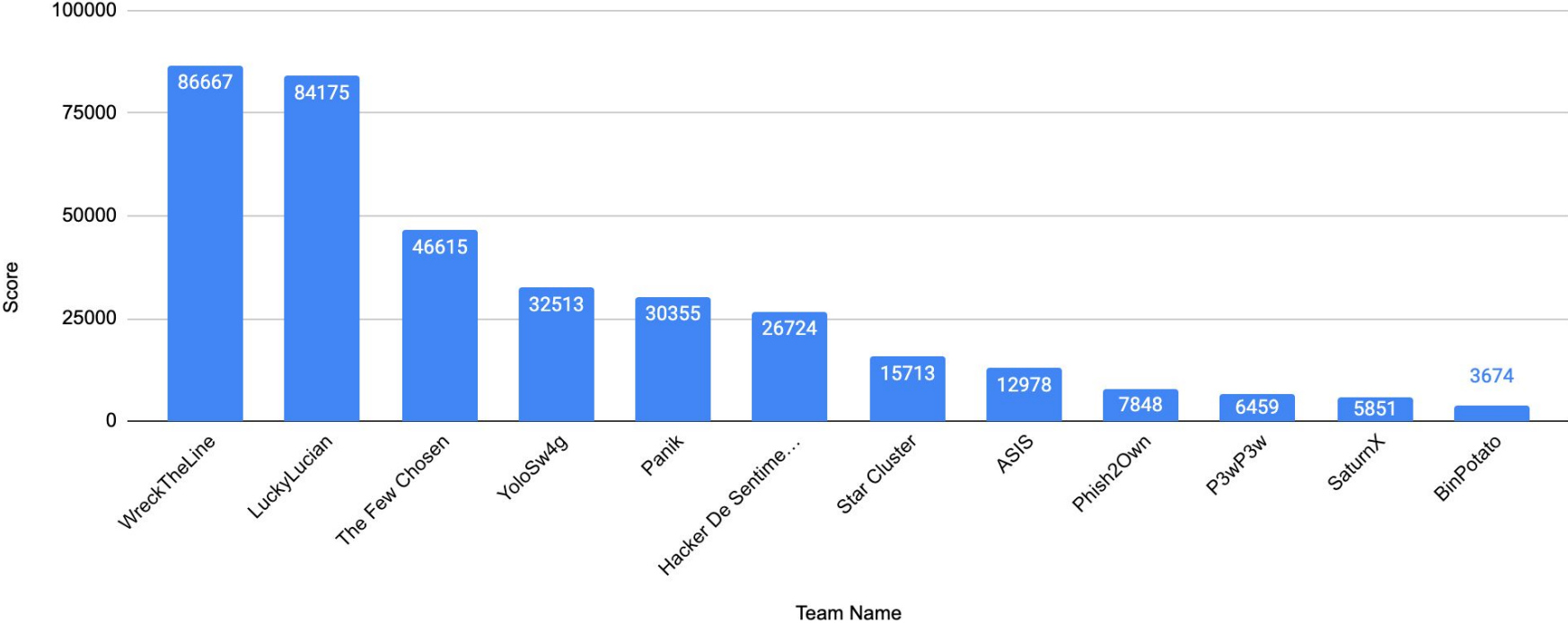




# Stats for nerds

- teams: 12
- total VMs: 30 (including infra)
- rounds: 240
- lowest score: 3,674
- highest score: 86,667
- stolen flags: 39,271 (roughly 80 flags / minute)
- uptime: 58% (career advice: don't apply for DevOps / sysadmin)

# Score vs. Team Name



# Next steps...

- more complex topologies (INT, EXT, DMZ 🤩 )
- modular vulnerability system (think Ansible roles)
- quicker deployment / configuration (Saltstack might be an option)
- Windows, Windows, Windows
- enterprise simulation (Active Directory FTW!)
- add more device types (routers, firewalls, switches, appliances, etc.)
- true self-service

# Thanks!

[sebastian.pitei@bit-sentinel.com](mailto:sebastian.pitei@bit-sentinel.com)