How (not) to organize a onsite CTF

Luca Campa, *University of Innsbruck*
Michele Lizzit, *University of Udine*
Matteo Paier, *IMT Lucca/University of Udine*

MadrHacks APS & University of Udine

MadrHacks is the CTF team of the University of Udine

Why creating MadrHacks APS? Strategic choice to simplify event organization and bureaucracy

University of Udine is partner with MadrHacks APS, and co-organizes our events

SnakeCTF

An event to spread cyber awareness and bring ~90 among the best hackers together; also by virtue of the prominent role that universities play within the National Cybersecurity Strategy

SnakeCTF Quals - Online - Remote - 700+ teams

SnakeCTF Finals - Lignano Sabbiadoro - EFA Village - 15 teams

SnakeCTF Finals 2025

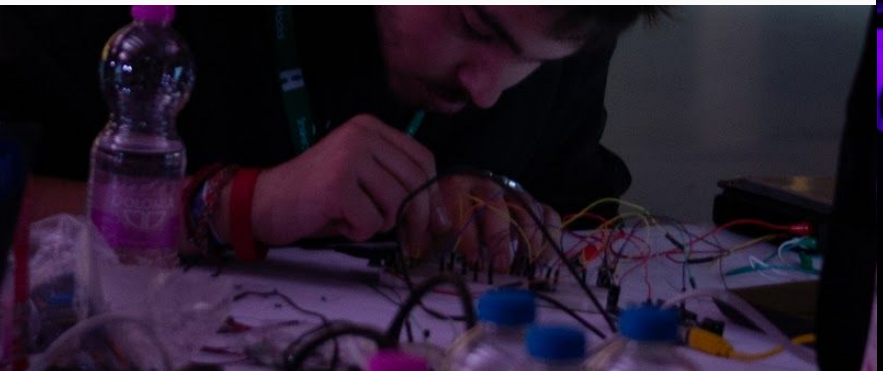
15 teams, 90 hackers from EU, Japan, South Korea, US & Kazakhstan

Main CTF

Jeopardy-style CTF

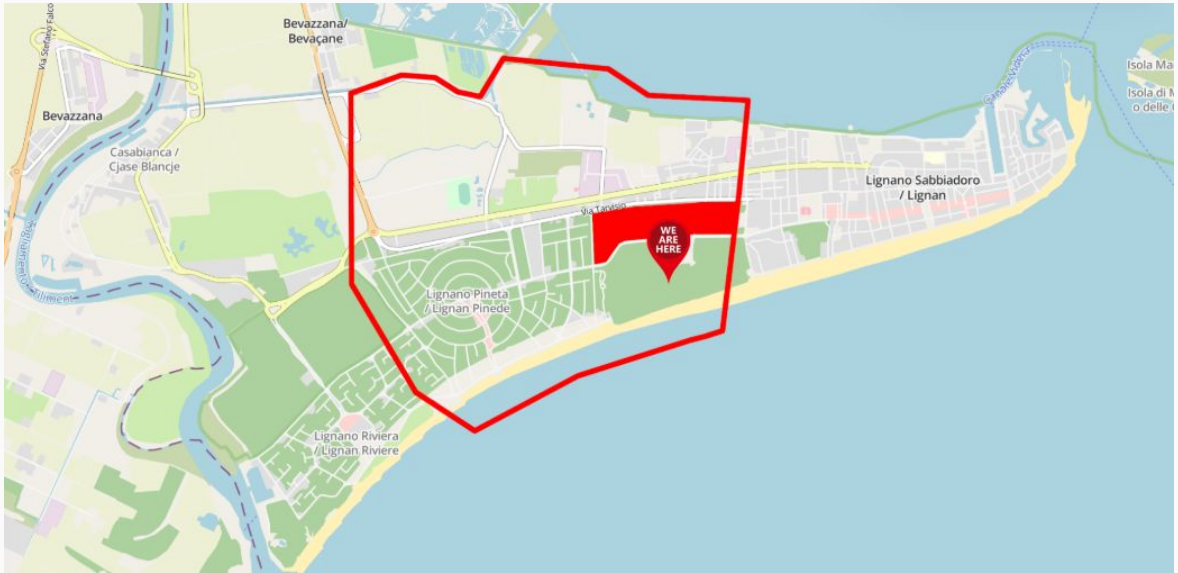
~15h. Played within the arena

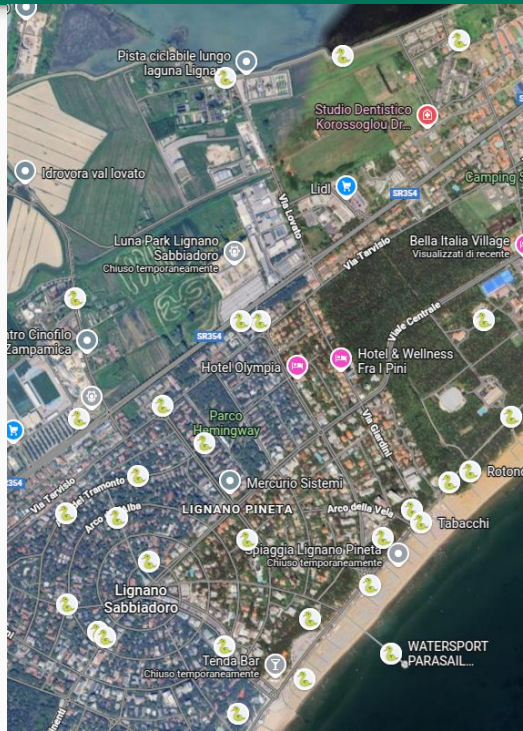
22 challenges incl. hardware



Real World CTF

Unique format. CTF in the real world. 30 challenges

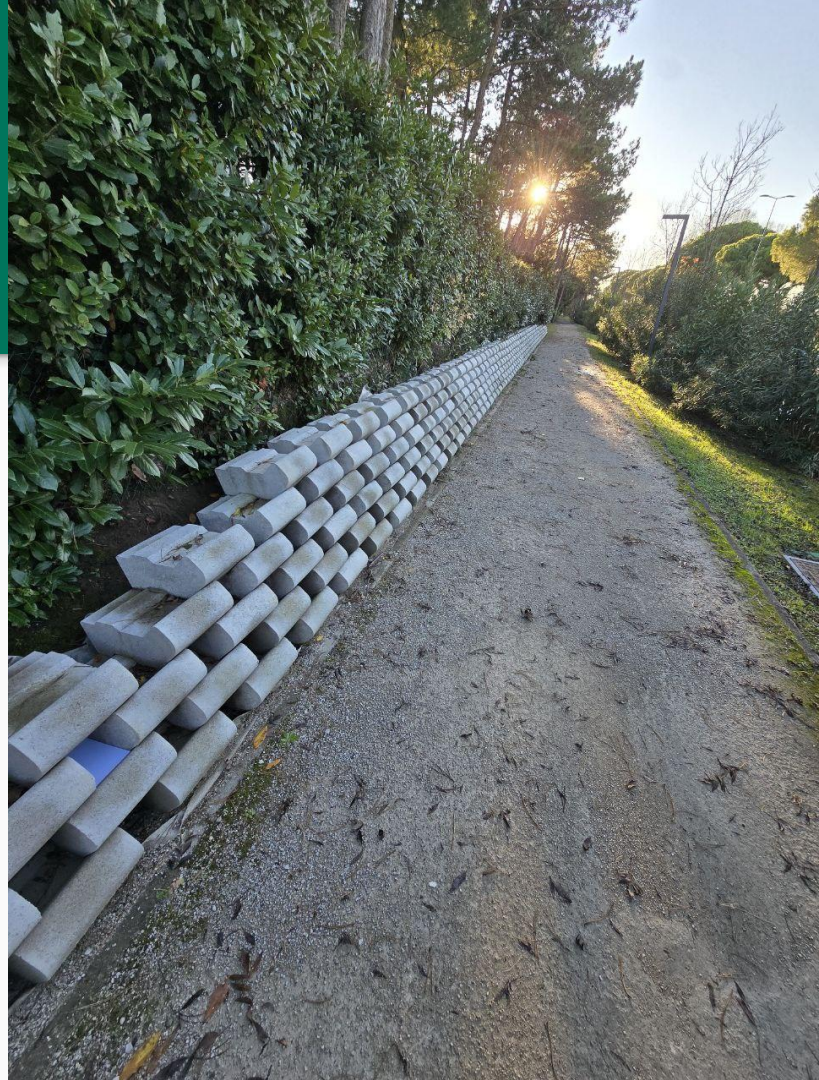




Real World CTF

First stage: recover the challenge location

- Geoguessing challenge
- Solve a traditional challenge
- Some other way



Real World CTF

From basic lockpicking to advanced RF hacking




Real World CTF

snakeCTF - couple

- Geoguess location of challenge 1
- Get location of challenge 2 via QR
- Reverse challenge 1 firmware, find a way to generate TOTP via BLE
- Insert TOTP in challenge 2 via WiFI
- Get the flag

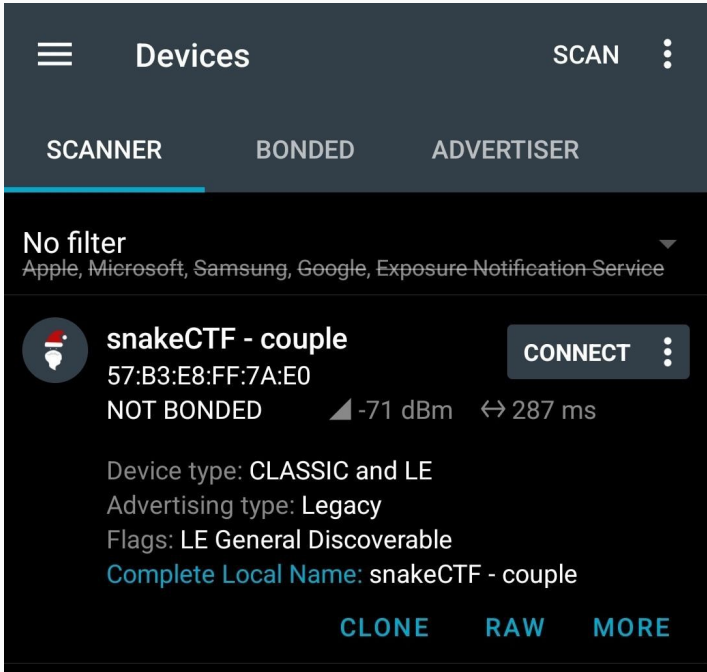
TOTP is valid for 8s only

Real World CTF

snakeCTF - couple

- Geoguess location of challenge 1
- Get location of challenge 2 via QR
- Reverse challenge 1 firmware, find a way to generate TOTP via BLE
- Insert TOTP in challenge 2 via WiFI
- Get the flag

TOTP is valid for 8s only



Real World CTF

Positive feedback. Players have enjoyed the format, despite some issues

Onsite CTF Infra

Two main sections:

1. Computing infra:
    a. CTF platform hosting
    b. Challenge hosting
    c. VPN
2. Onsite support infra
    a. Electrical system
    b. Connectivity
    c. Logistics

Equally important!

Computing infra

All in cloud: this year we used **GCP** (total cost: ~450$/500$ grant). Why?

The Quals infra cannot be on-premise. In the Finals we allow 6 persons/team onsite, but we have no limit for remote players. So we can use a very similar platform.

Used **Kubernetes** for the most part. A single out-of-cluster VM has been used for the VPN concentrator (but connected on the same VPC).

Kubernetes cluster

We use different VMs for different tasks:

- 2× n2-standard-4 for **management**
- 2-4× (autoscaling) n2-standard-4 for the **challenges**
- 1-12× (autoscaling) t2d-standard-4 for **spawned instances**

We use **Terraform** and **Ansible** for the provisioning of the entire infra: from the VM creation to the DNS records.

Management infra

The infra is **custom made** for SnakeCTF.

We use **Traefik** as the in-cluster reverse proxy/load balancer.

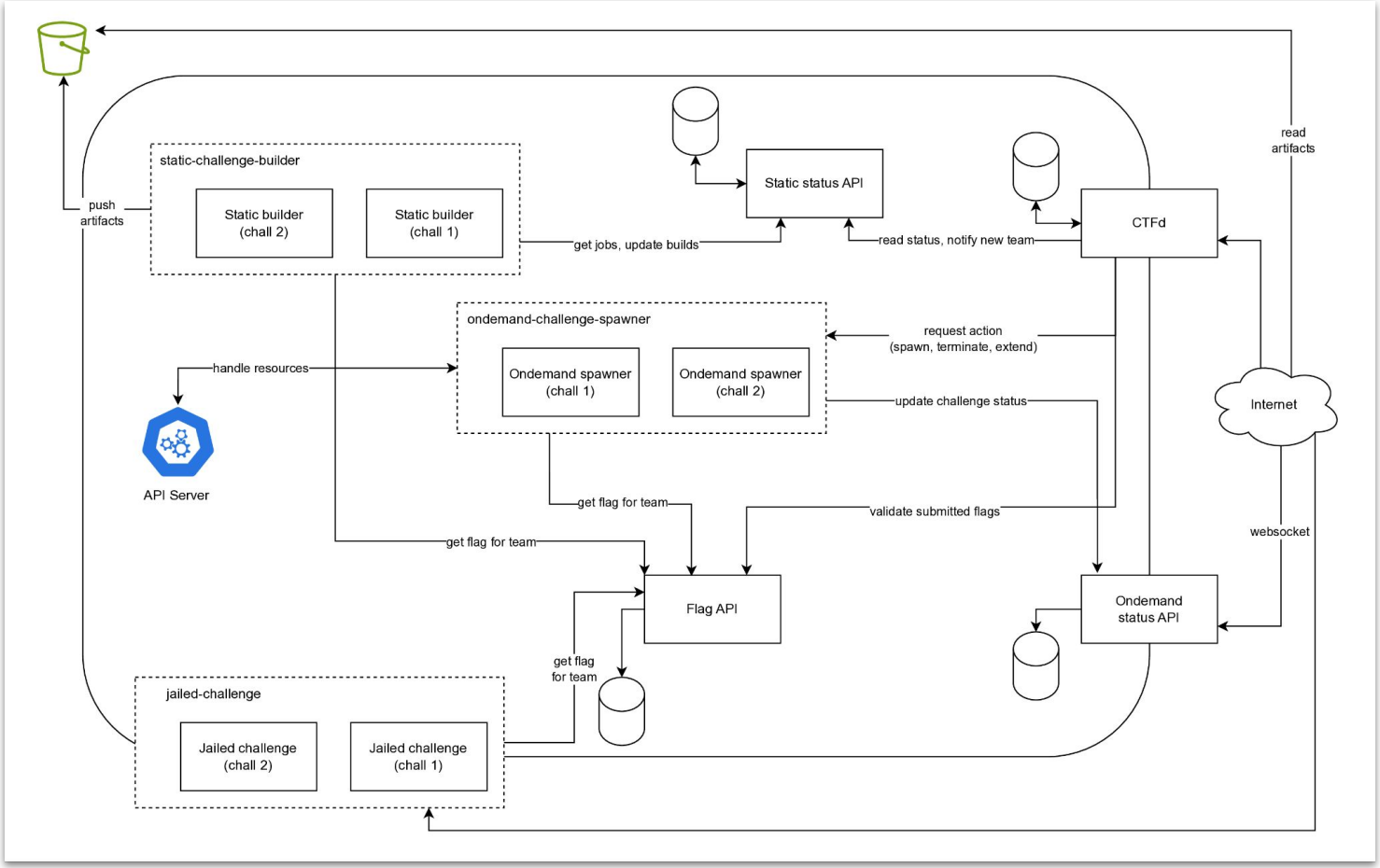
We use **CTFd** as the CTF platform, but we developed a lot of different **plugins** and **microservices** for flag management.

We want to give **different flags to different teams**, to detect (basic) flag sharing.

Custom flags

We have 4 types of challenges:

1. **standard**: the usual, one flag for everyone
2. **static**: for challenges with attachments. We build the attachment with a custom flag for every team
3. **jailed**: for remote challenges where jailing is possible (e.g. pwn). The jail gets the team's flag and passes it to the jailed app
4. **ondemand**: for more complex remote challenges (e.g. web). An instancer deploys a new instance for each team



A simplified view of the k8s infra

VPN

Most of the cluster is reachable only from the competition VPN.

A VM acts as a **concentrator** to allow access to the network.

We use pure **WireGuard**, with a single **iptables** rule to allow traffic only towards the cluster ingress IP.

This is done to prevent players using the competition VPN as a public VPN with unrestricted remote access.

Onsite support infra

Developing (and deploying) the infra for a **onsite event** is not trivial.

This is true in particular for a “computing” event, where a **good connection and power source** are expected.

Why not **outsourcing**?

We were unable to find a company able to meet our performance and reliability requirements.

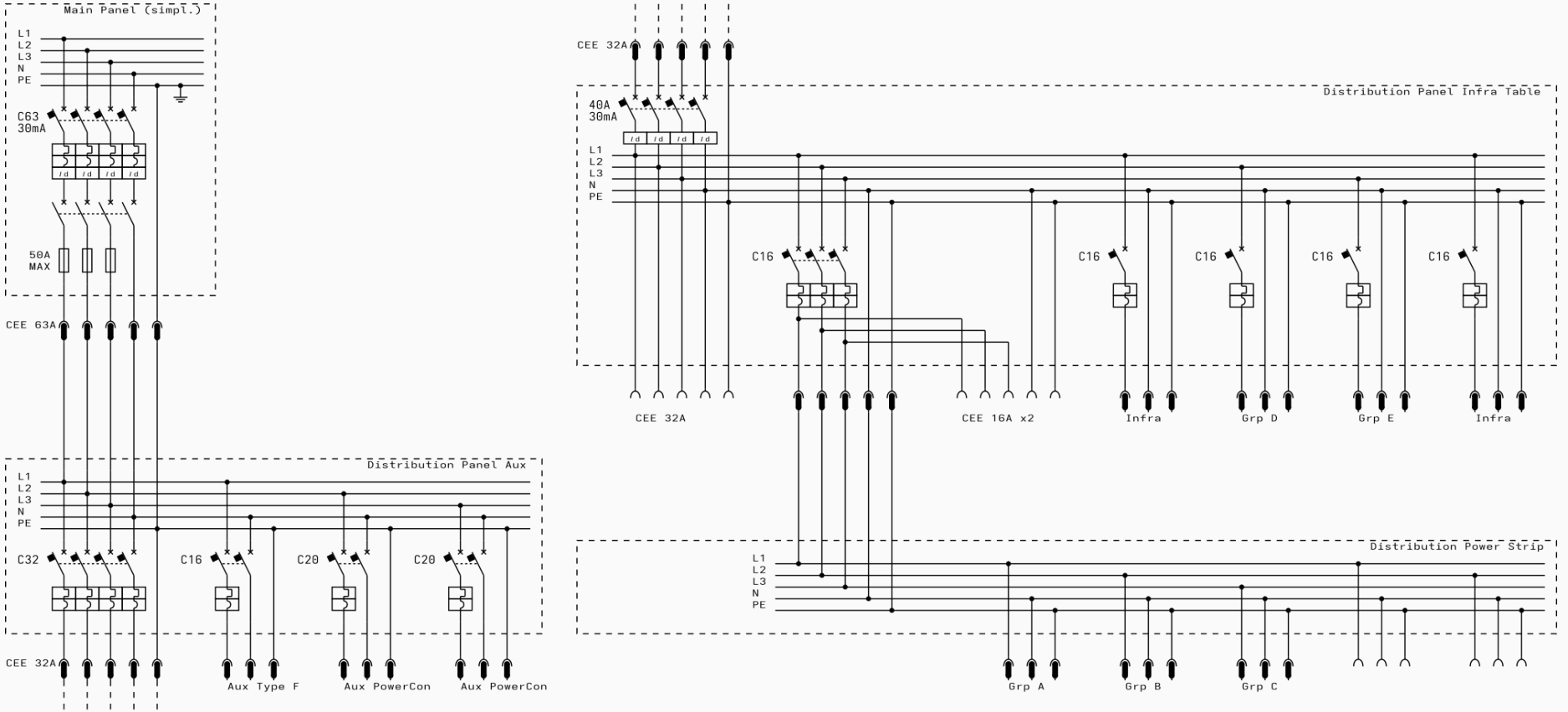
Electrical system

Computers can consume a lot of power.

We want to **guarantee** at least 1kW/team (~150W/person), 3kW for the infra and staff, 3kW for catering, 5kW for lights and misc devices.

Total: 26kW = ~37,5A at 400V

The deployed infra is capable of delivering **~34kW**.



Schematic of the deployed electrical system

Connectivity

The network must be **highly segmented**:

- 1 VLAN/team
- infra VLAN, admin VLAN, staff VLAN
- WiFi VLAN…

We allocate **10.30.0.0/19** (8,192 IPs) for the competition network.

The **uplink** is **~1Gbps** symmetric.

Also, we have a (hot) **fallback** connection via 5G cellular network.

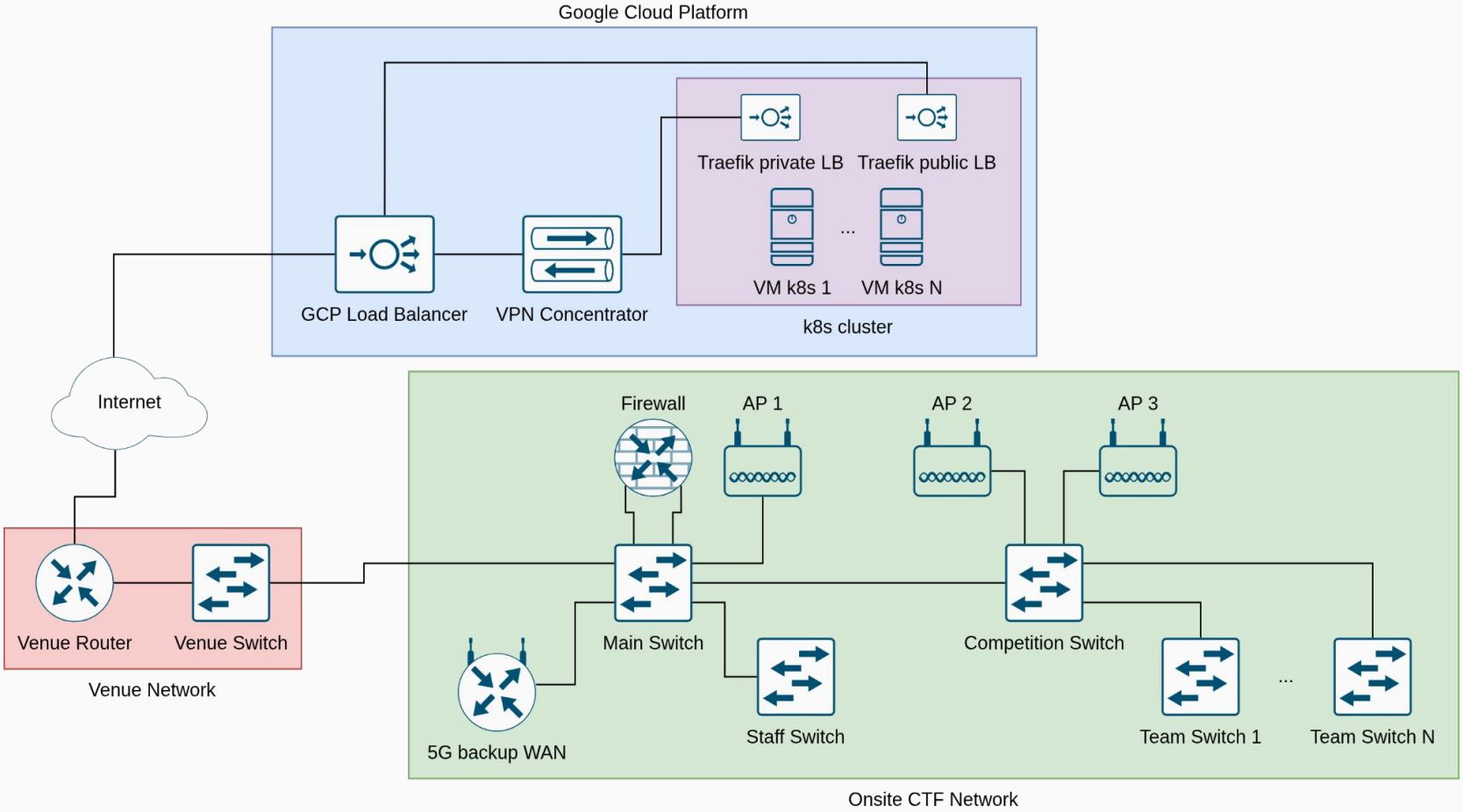
Connectivity

The firewall/router is **virtualized** (a OPNSense VM with NIC passthrough on a Proxmox VE host).

We provide (guest) **WiFi** connectivity in the game arena with 3 APs, on 2,4GHz, 5GHz and 6GHz with **manual band allocation**.

Singlemode fiber is used to connect the main switch with the central competition switch, since the cable is promiscuous with the 400V backbone.

We use **two public IP** to **NAT** different kind of traffic: player and staff/infra.

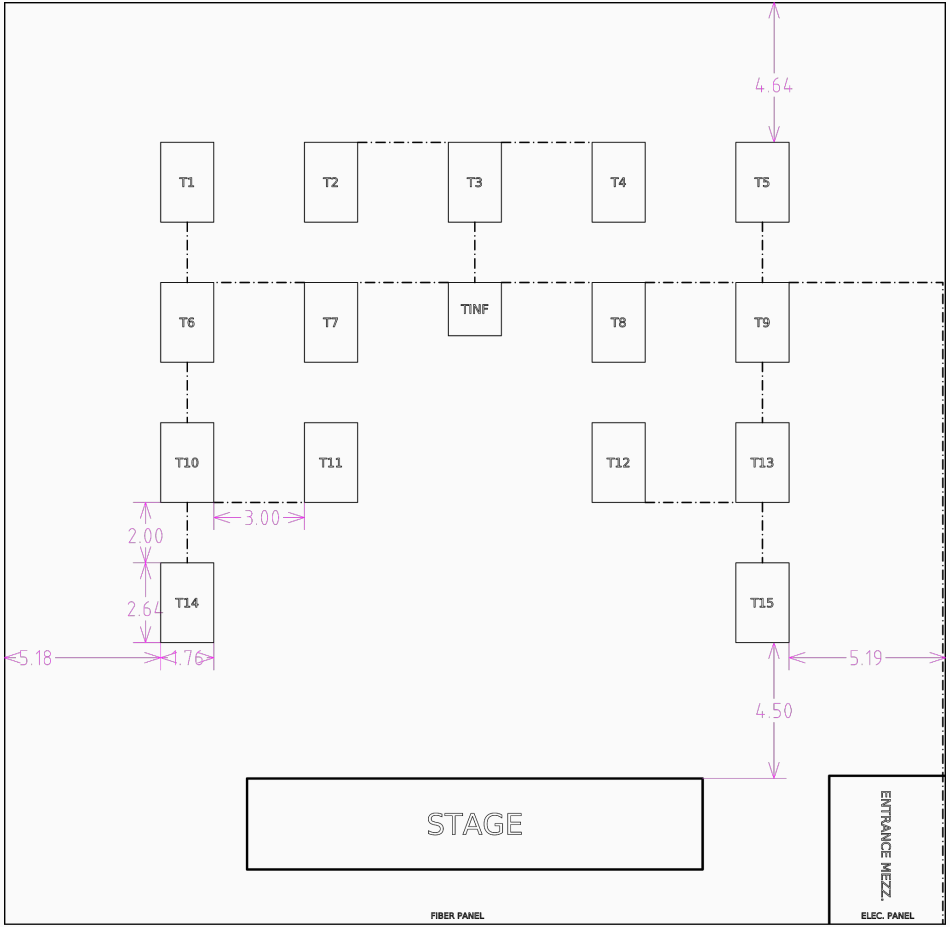

Google Cloud Platform
Traefik private LB
Traefik public LB
VM k8s 1
...
VM k8s N
k8s cluster
GCP Load Balancer
VPN Concentrator
Internet
Firewall
AP 1
AP 2
AP 3
Venue Router
Venue Switch
Venue Network
Main Switch
Competition Switch
5G backup WAN
Staff Switch
Team Switch 1
...
Team Switch N
Onsite CTF Network

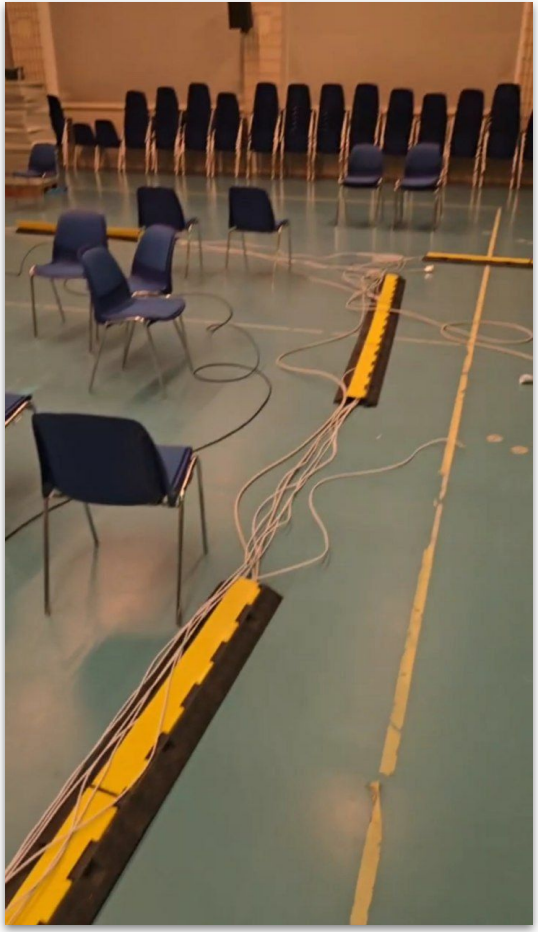
Logistics

After the planning, a lot more still needs to be considered:

- Transport
- Deploy wiring, devices, tables…
- Coordinate the arrival of the players with the venue
- Test everything

To ease this, we prepare detailed **schematics** and **checklists** during the planning phase.





The floor plan with the deploy dimensions for the tables and cable ducts

Inventory

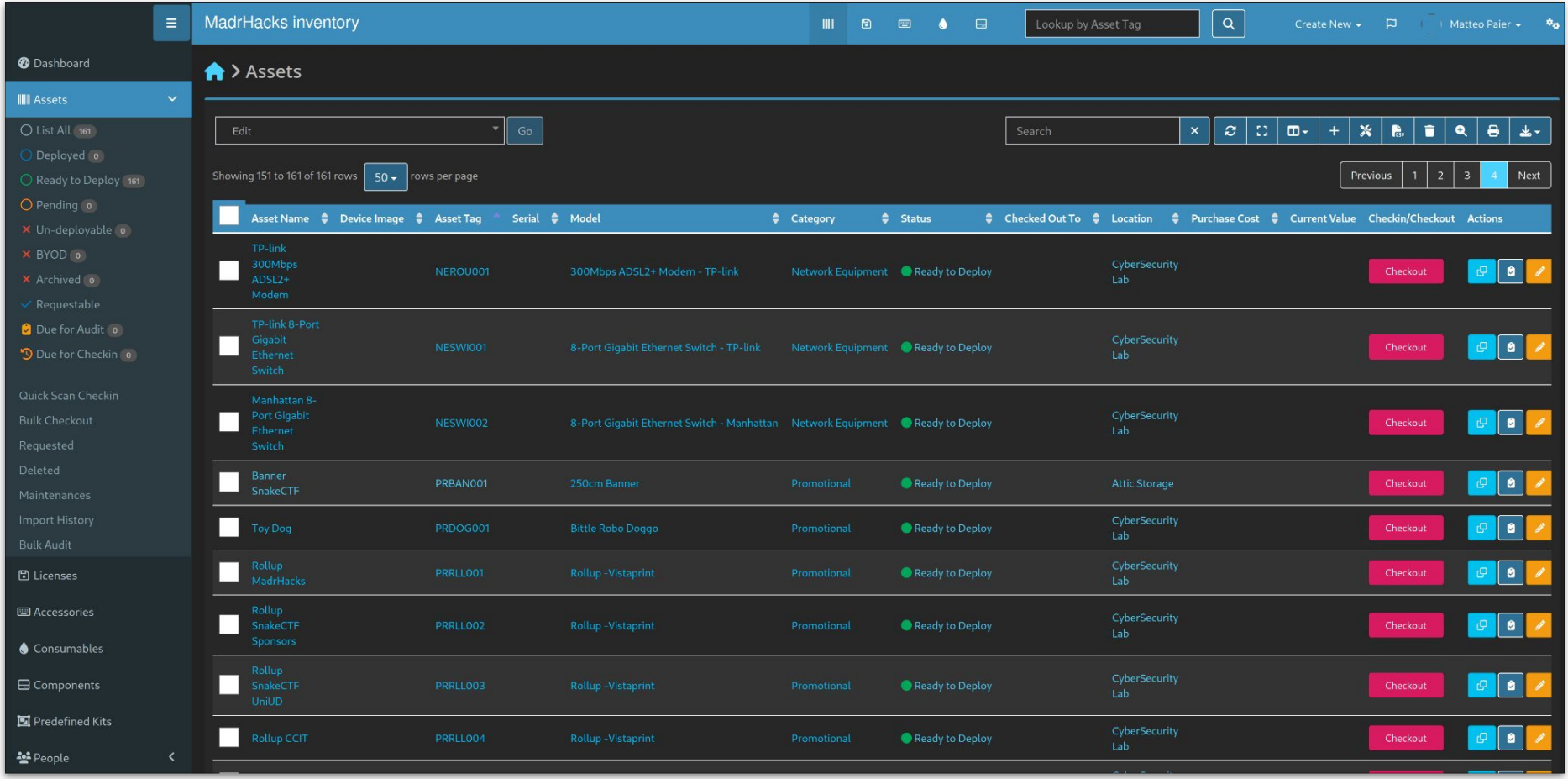
During onsite events, you will[1] lose stuff.

How to counter that? (Or at least know what you lost?)

Label everything that moves out of storage and track its location.

We use Snipe-IT to **track assets** (161 at the moment, several hundred more not yet labelled). We use Data Matrix codes for quick scanning.

1: $P_{losing\_stuff} > 1 - \varepsilon$



Snipe-IT used as asset/inventory manager

(this is actually compliant with the limitations in the vehicle registration certificate)

How to transport all the material, when you discover you underestimated the amount?

Inspections before the event

- The entire venue (total capacity 3000 guests + staff) was connected on a 500Mbps symmetric connection. This is clearly insufficient for a CTF. So we coordinated a **bandwidth increase** with the ISP. Also, knowing this, we prepared a **backup WAN** on a 5G cellular connection.
- We discovered the data wiring at the venue was **broken**, so we asked for a fix. Fiber was deployed from the venue rack to the game arena.

Inspections before the event

- Inspecting the electrical panel we discovered some **faulty** RCDs. The issue was promptly fixed by the venue.
- We checked the fuses in the electrical panel to ensure we had spares ready

What we learned infra-wise

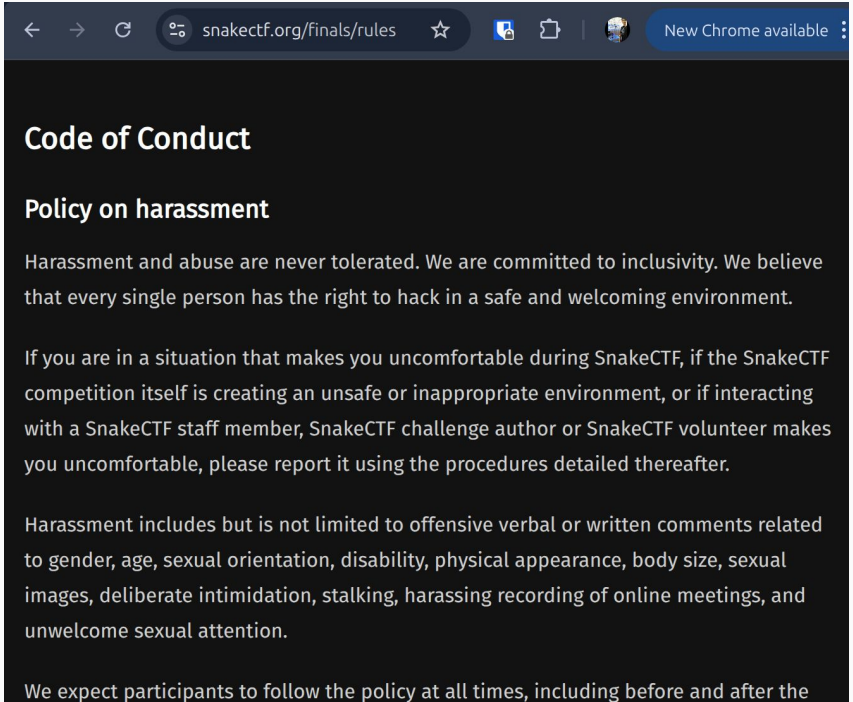
- **Test** the connectivity more thoroughly (apparently the Discord CDN was unreachable)
- **Configure** and test all the equipment before arriving at the venue
- **Label** everything!
- Surveys/**inspections** long **before** the event
- **Coordination** with the ~~venue~~ **technical partners** of the venue

Code of Conduct

- We aim for a healthy and safe environment for everyone
- Hotline for harassment reporting & 2 point of contact; allows us to monitor
- In 2025 we adopted a new, stricter code of conduct



Code of Conduct



Code of Conduct

- We aim for a healthy and safe environment for everyone
- Hotline for harassment reporting & 2 point of contact; allows us to monitor
- In 2025 we adopted a new, stricter code of conduct
- Code of Conduct significantly improved gender diversity among players
- Despite this, we receive at least 1 harassment report every year

Ongoing issues

- Lack of human resources (volunteers, challenge authors, etc.)
- Same issue as many other small teams
- Currently struggling to organize SnakeCTF 2026
- Partnership with other Universities is the only way forward

Thank you for your attention!

Any questions?

Luca Campa, *University of Innsbruck*
Michele Lizzit, *University of Udine*
Matteo Paier, *IMT Lucca/University of Udine*

info@madrhacks.org