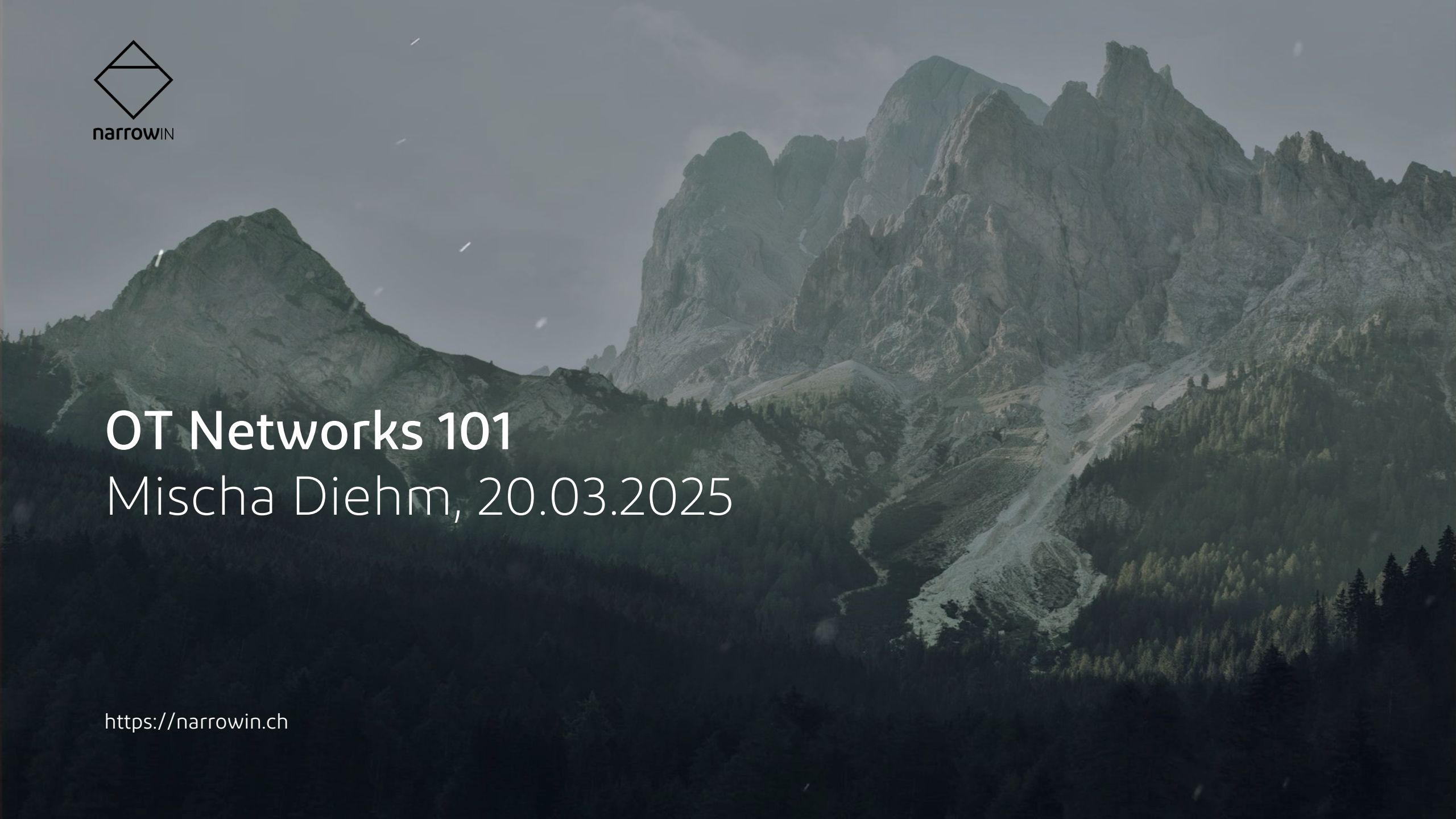


narrowIN

OT Networks 101

Mischa Diehm, 20.03.2025

https://narrowin.ch

Who?

Mischa Diehm

- Founder of narrowin
- Network design and development
- Computer and network infrastructure

narrowin

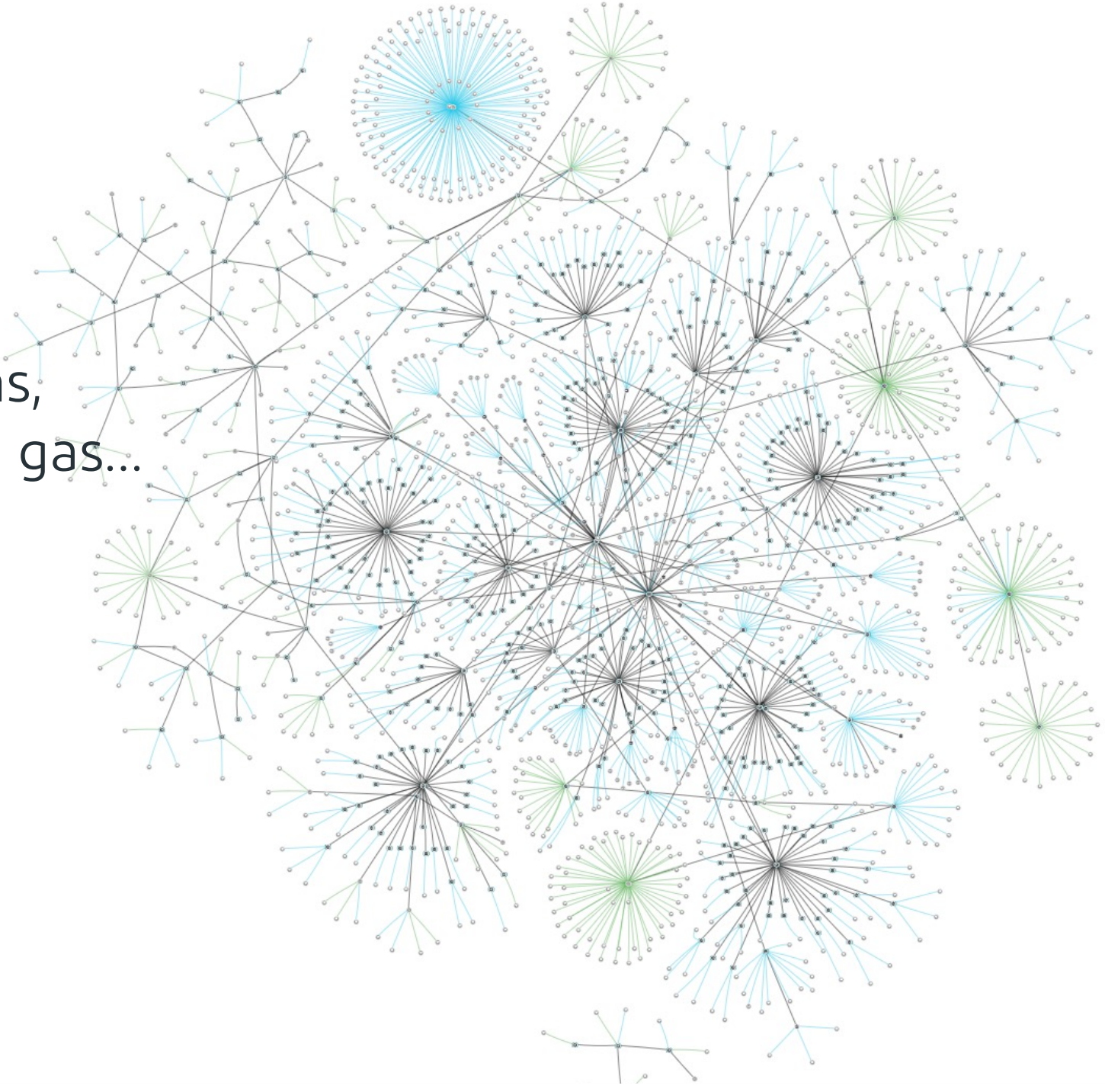
- Networking and security
- Micro-/Endpoint segmentation
- Lightweight Network Explorer

https://demo.narrowin.ch

SWISSGAS eniwa EnBW Kernkraftwerk Gösgen axians

Manufacturing, smart metering, trafo stations, district heating, water, gas…

OT / IoT Networks are growing and growing



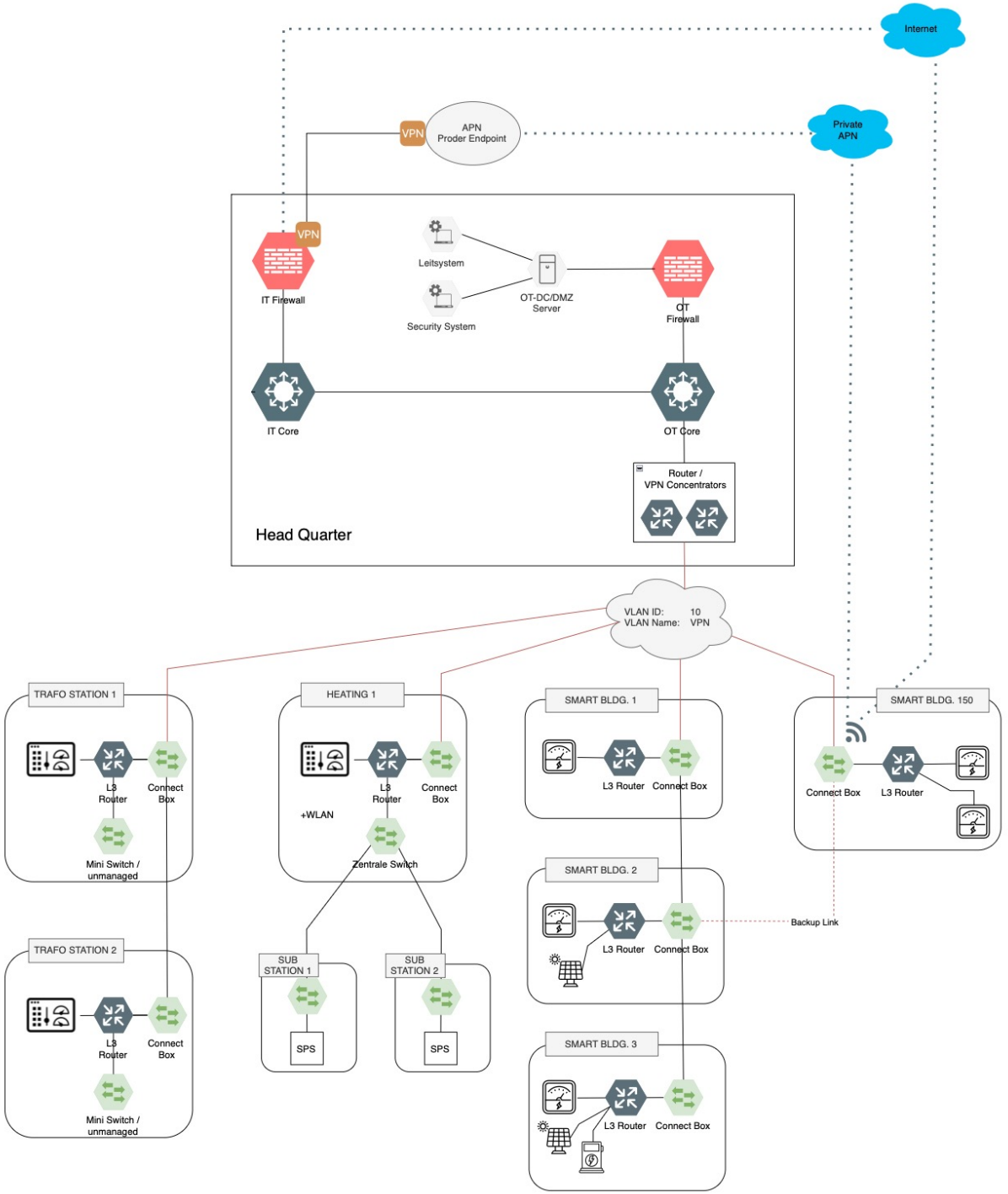
OT Network Design seems very clear on first sight...

Design Principles:

- ✓ Resilience
- ✓ Fault tolerance
- ✓ Bandwidth management

Operational/Security Best Practices:

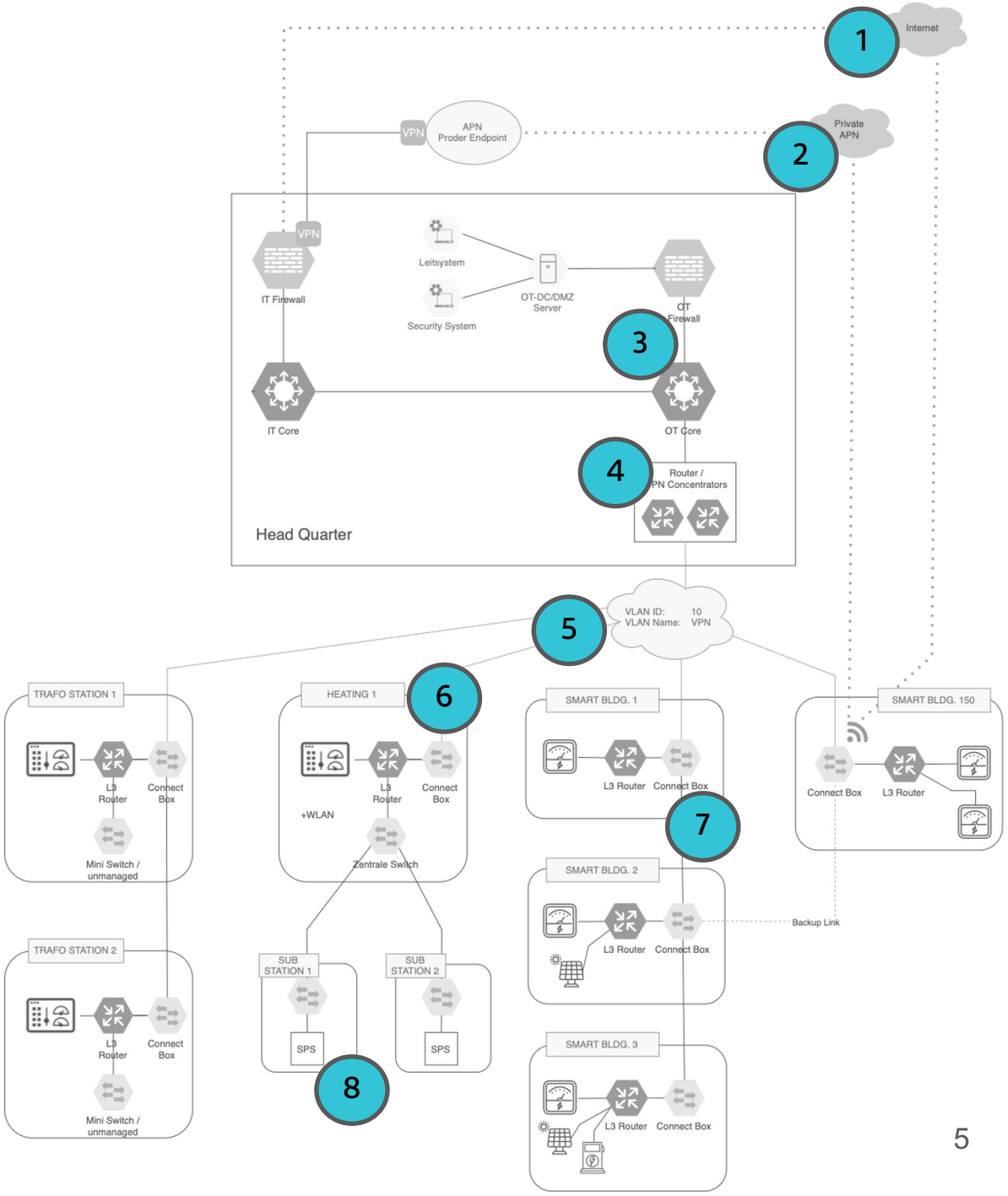
- ✓ Network segmentation
- ✓ Encryption in transit
- ✓ Continuous monitoring



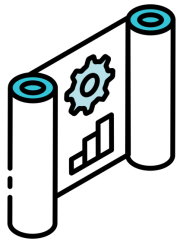
… or is it?

1. How can we ensure save remote access?
2. Do we need a private APN?
3. Do we need a dedicated OT Core?
4. How are these networks routed?
5. Do I need decentral firewall features?
6. How can I homogenize the setup across use cases?
7. How do I minimize the blast radius on layer 2?
8. How do I micro-segment critical systems?

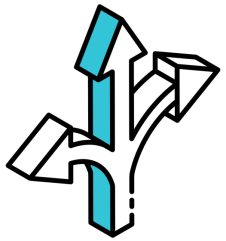
… etc.



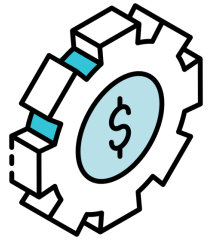
Let us zoom in on some topics



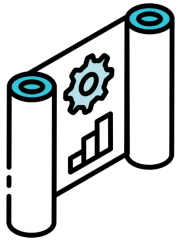
Secure Config



Segmentation

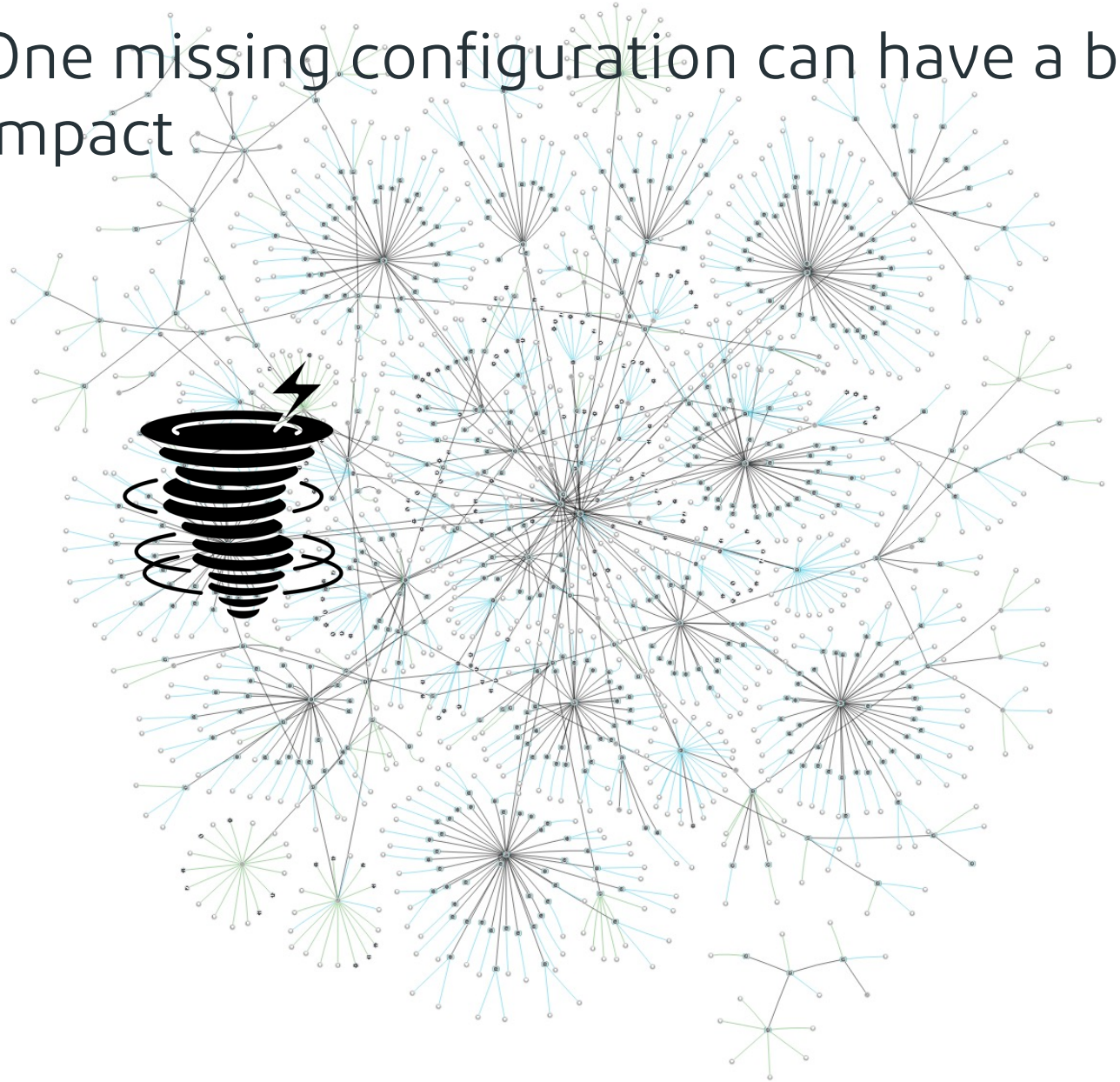


Network Automation



Secure Config

One missing configuration can have a big impact



Example: Spanning Tree

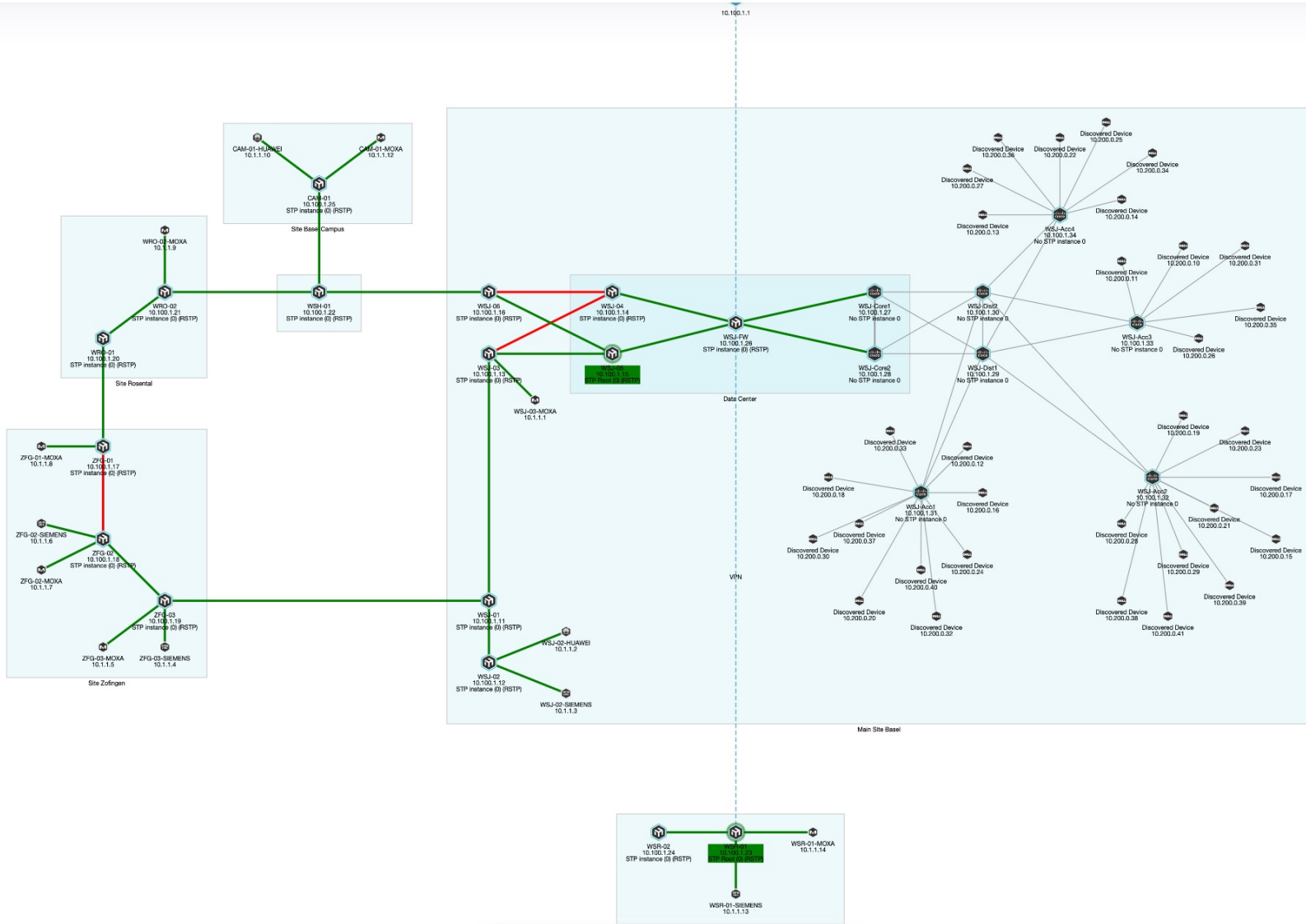
- Spanning Tree Protocol is vital in L2 networks
- Configuring STP for reliability and fault tolerance
- Avoiding misconfigurations that can cause downtime or network loops

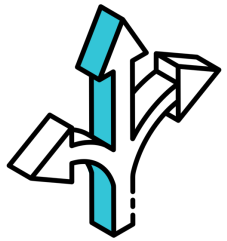
Network 2 (with Layout) | live

narrowIN

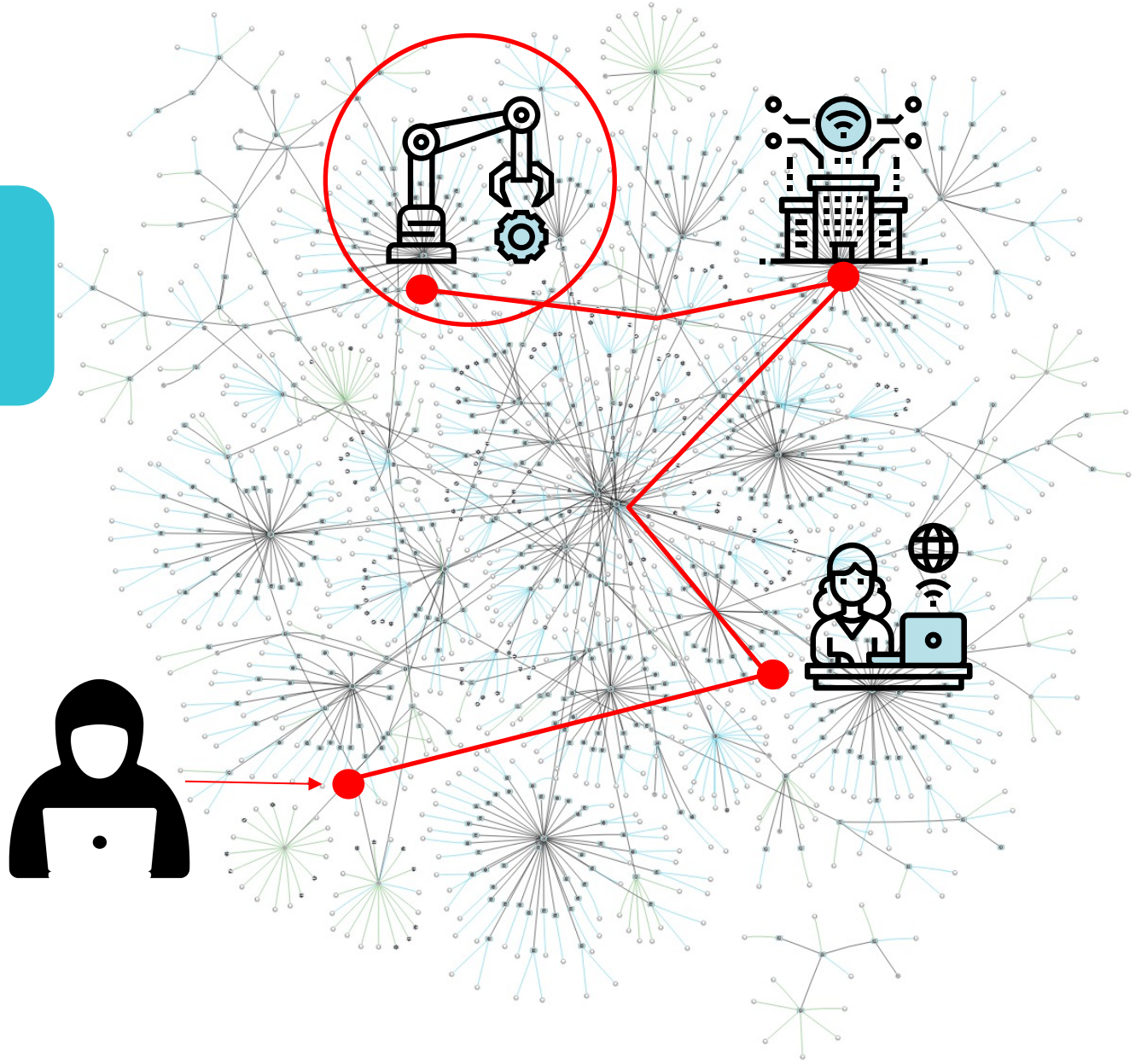
Netmap | Inventory | Segmentation | History | Assessment

View: Spanning Tree | Instance/VLAN ID: 0 | All | Search ...



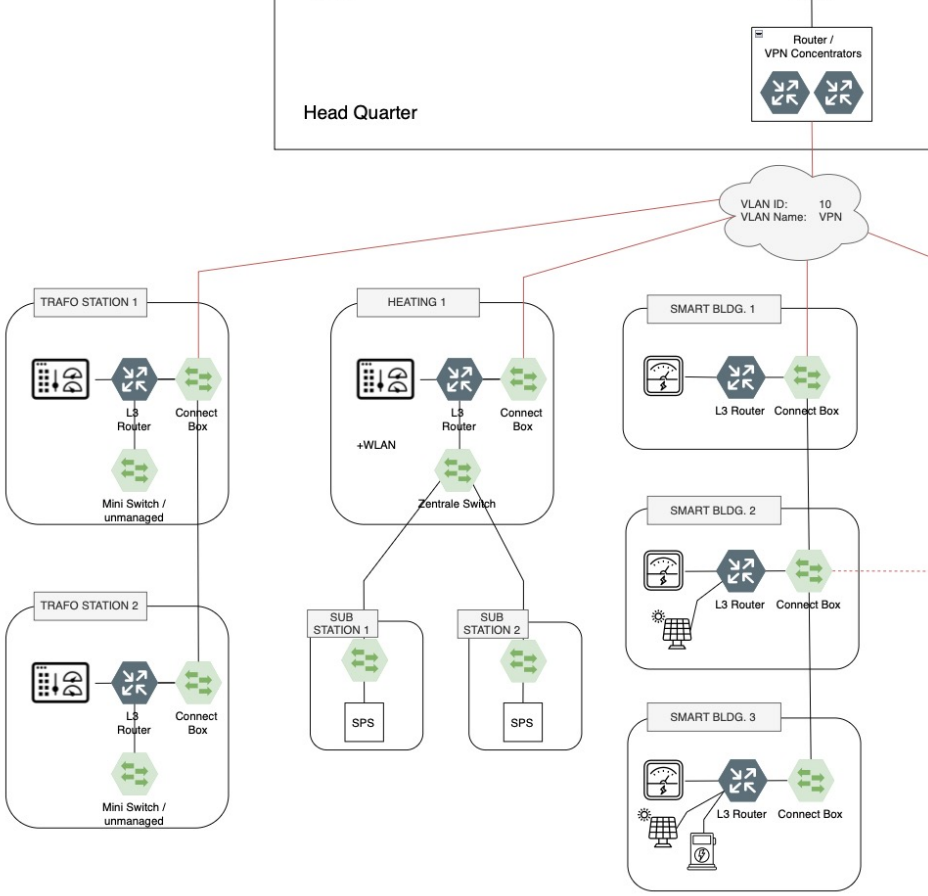


Segmentation



Example: Isolating Remote Sites

- Separating remote locations into distinct L3 domains
- Layered security measures (VLANs, VRFs, VPNs, Firewalls)



L2 Security

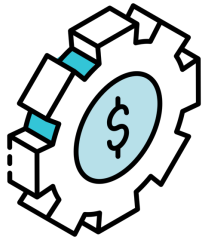
1. Minimize L2 attack vector (MiTM, ARP Spoofing, ...)

L2 Blast Radius

1. Limiting the scope of network faults and security incidents
2. Preventing a single point of failure from spreading across the network

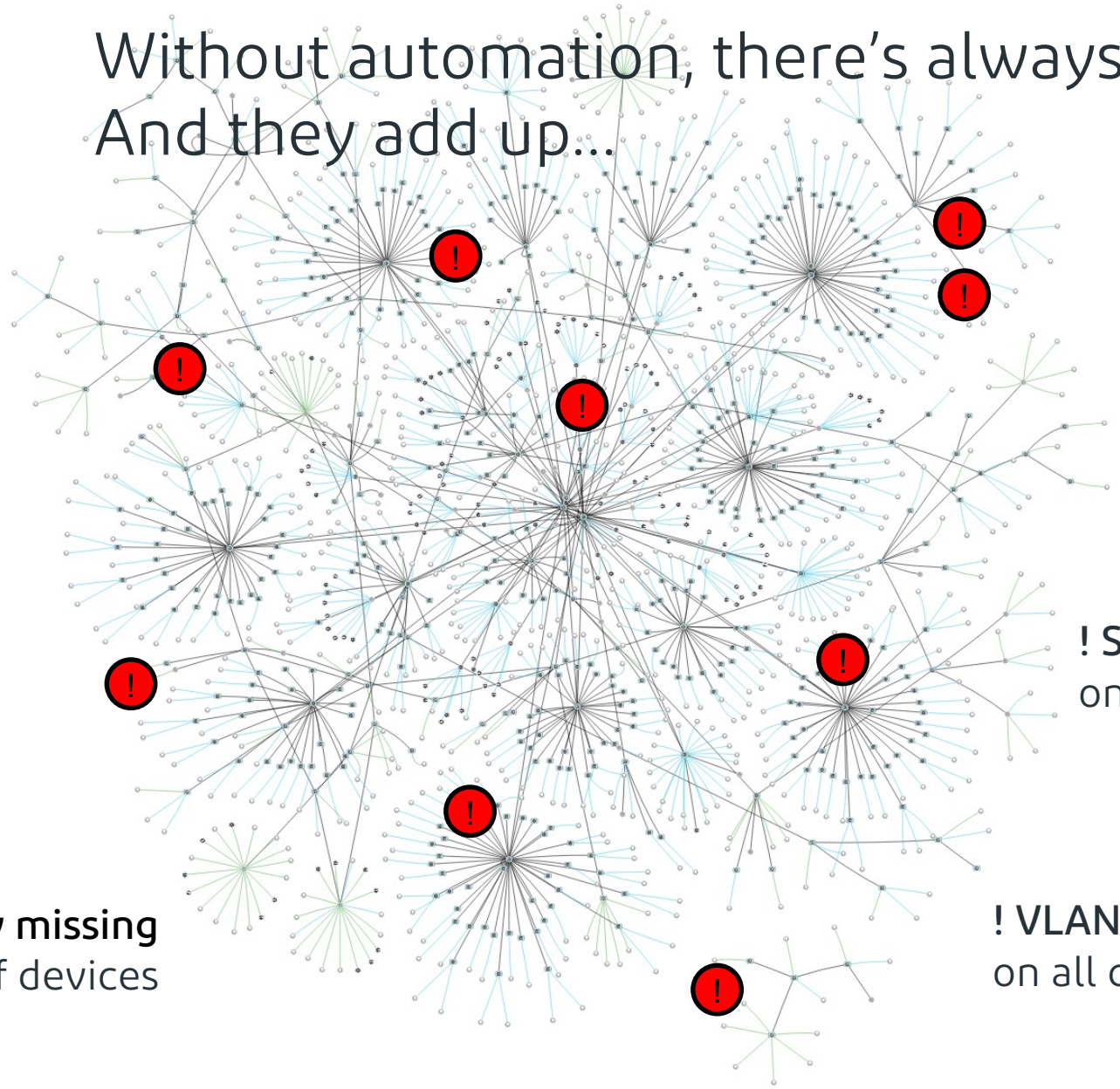
Preventing Lateral Movement

1. Micro-segmentation to protect critical OT assets (PLCs, RTUs) inside the locations
2. Using local ACLs and central firewalls between different segments



Network Automation

Without automation, there's always gaps. And they add up...



! NTP not configured
on 5% of devices

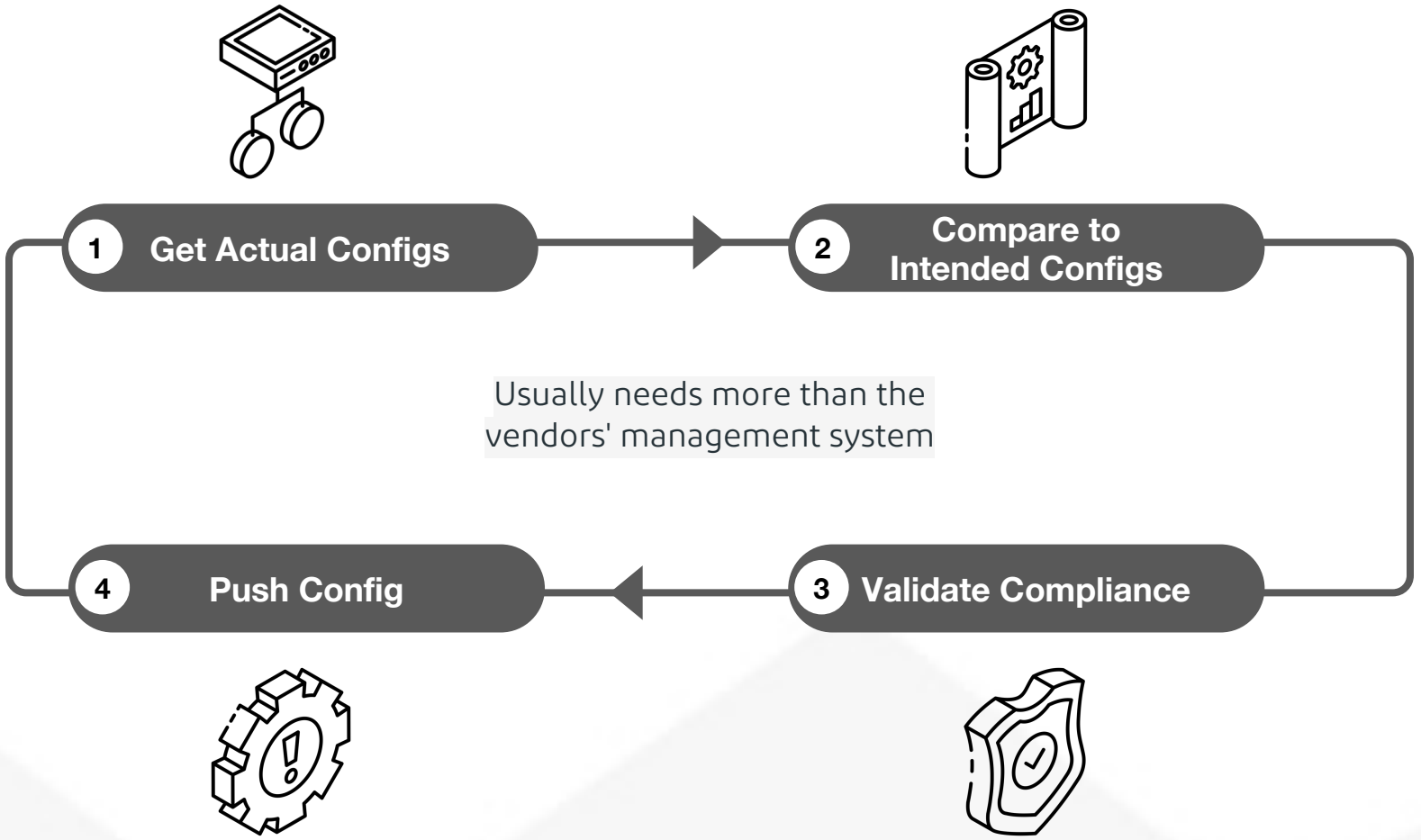
! Reversible Password encryption
on 16 devices

! STP misconfiguration
on 4 devices

! Port Security missing
on 20% of devices

! VLAN 1 not disabled
on all devices

Automation allows to detect and fix these blind spots, avoiding “configuration drift”



Final thoughts

These topics are not rocket science, but …

- some of them are **painful and expensive to adjust ex post**
  (e.g. segmentation)
- some of them are **necessary to scale without running into personnel problems**
  (e.g. laying the foundation for automation)
- some of them are **easily forgotten but can disrupt your whole network**
  (e.g. not properly configuring STP)