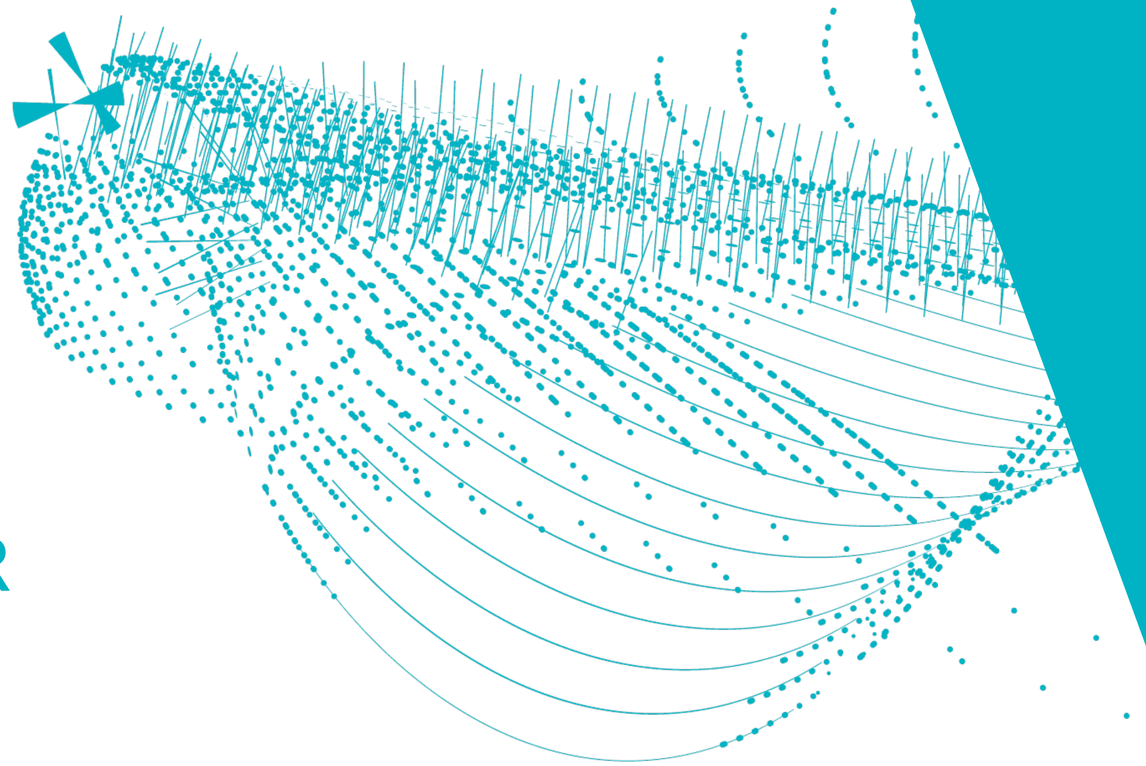
Nikhef



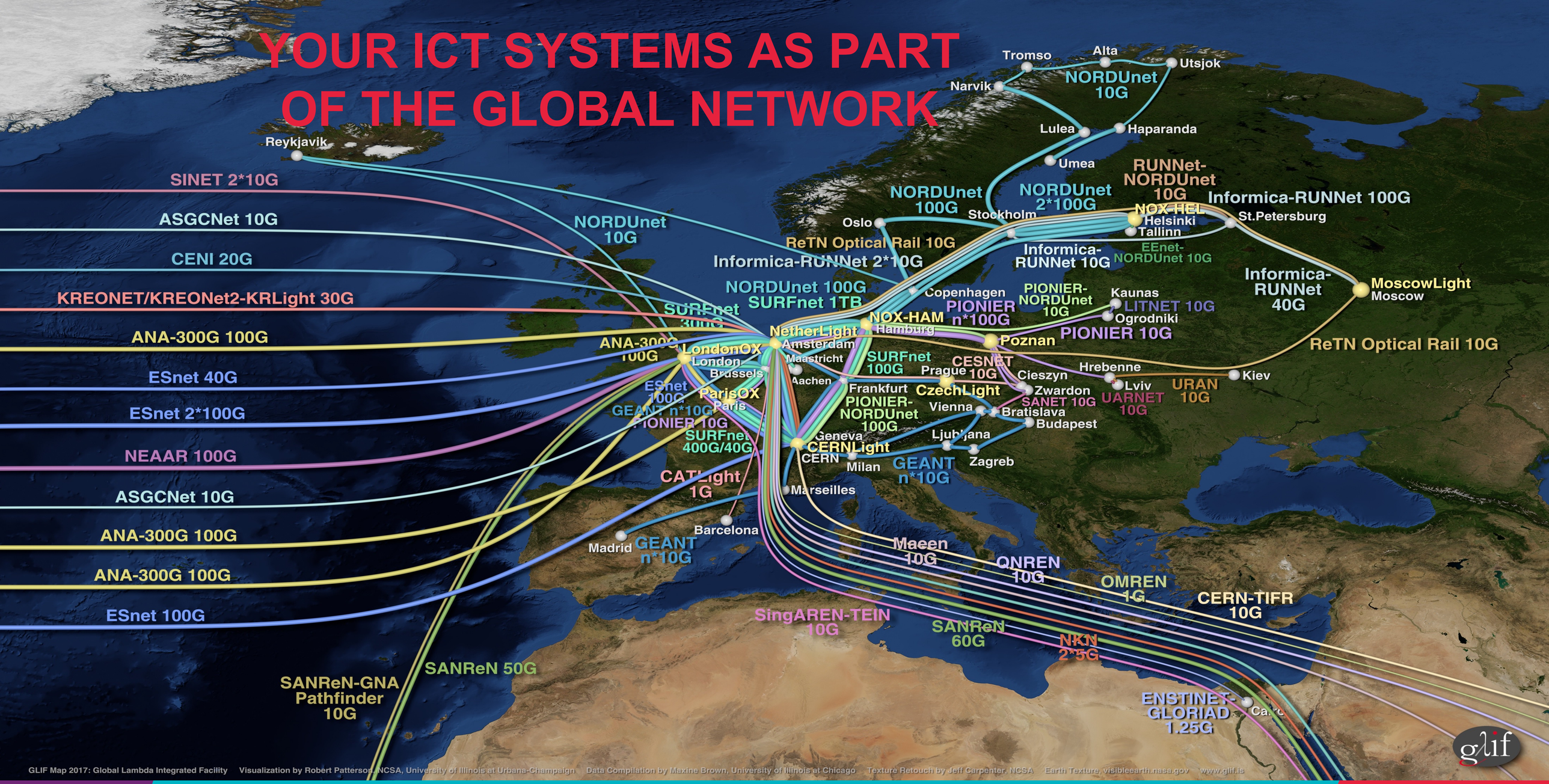
NIKHEF CSIRT
SECURITY OPERATIONS CENTER

SECURITY MONITORING AT SCALE

Sil Westerveld
20241016

OPERATIONAL SECURITY, FOR WHAT ACTUALLY?

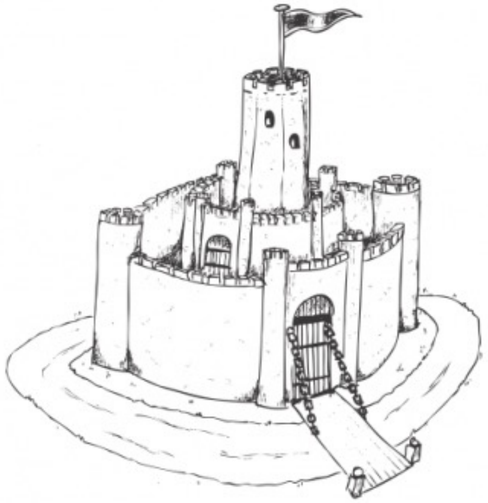
YOUR ICT SYSTEMS AS PART OF THE GLOBAL NETWORK



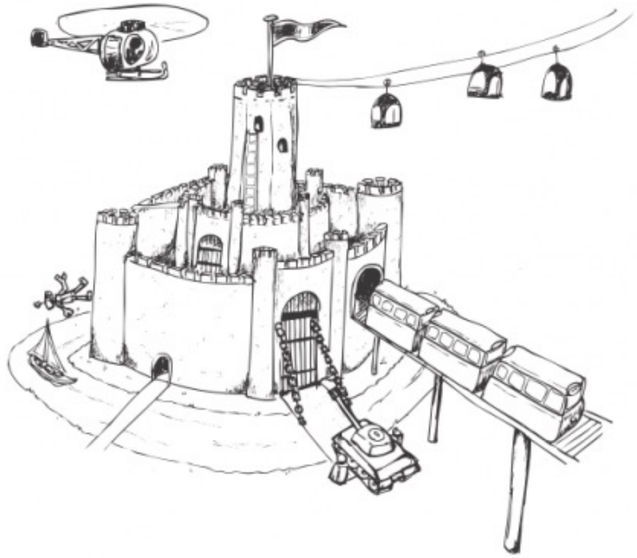
CASTLE MODEL IN IT SECURITY

DOES THIS REALLY WORK IN OUR ENVIRONMENT?

Castle Model of Security



Castle Model in Reality

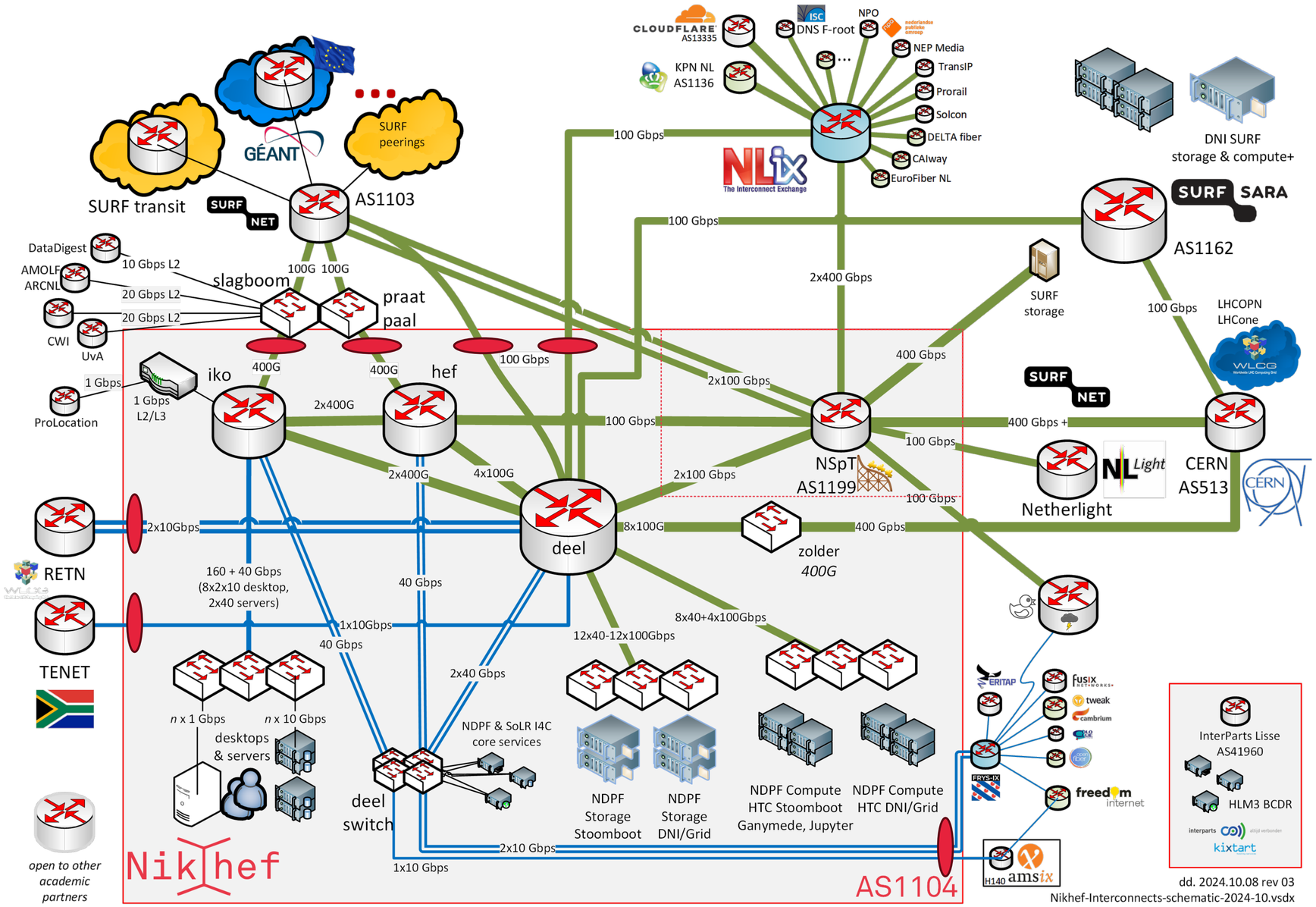


LEUPRECHT, C., SKILLICORN, D. B. & TAIT, V. E. (2016). “BEYOND THE CASTLE MODEL OF CYBER-RISK AND CYBER-SECURITY.” GOVERNMENT INFORMATION QUARTERLY, 33(2), 250-257.

NIKHEF SOC

SECURITY OPERATIONS CENTER

A collection of
processes, people and technologies
that support the cybersecurity staff of
an organization in **identifying**
anomalies in their environment and in
successfully **investigating security**
incidents



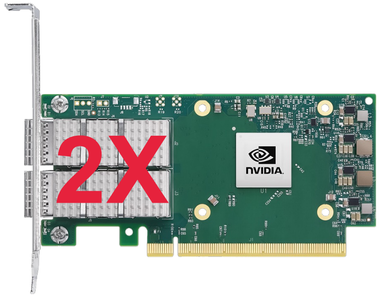
Nikhef CSIRT – Security Operations Center – Security Monitoring at Scale

Nikhef

INFRASTRUCTURE

2X

2X



zeek

8X

PROXMOX

APACHE kafka™

logstash

6X

elasticsearch

WHAT DOES THIS PROVIDE US WITH?

real-time situation monitoring

inspection of network traffic

alerting based on IOCs

historical data

network traffic

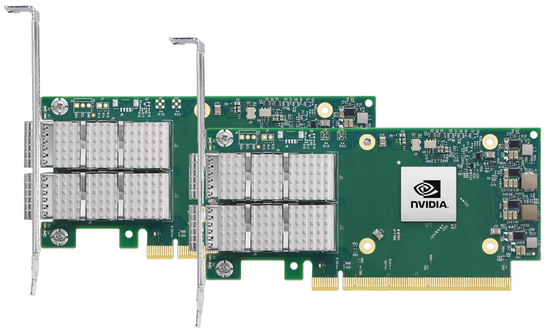
logs of systems on our network

HOW DO WE KNOW INDICATORS OF COMPROMISE?

zeek

MISP TO ZEEK EXPORT

MISP
Threat Sharing



SYNC

SURF CERT

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

CERN

THREAT fox
by ABUSE.ch

WHAT MAKES IT “AT SCALE”?

zeek

elasticsearch

3.2Tb/s throughput *

up to 2.38 Bpps *

* times two

easily does 100Gb/s

could in theory inspect taps at rates up to 400Gb/s

inspection based on ~40K MISP events

~14TB hot (SSD)

~220TB cold (HDD)

~600GB per day

~52 billion docs

SOME AUXILIARY TOOLS & SERVICES

Attack surface monitoring

- CESNET Pakiti
- Tenable Nessus
- Shodan.io

Manual lookups for reporting

- Kibana
- Netdisco