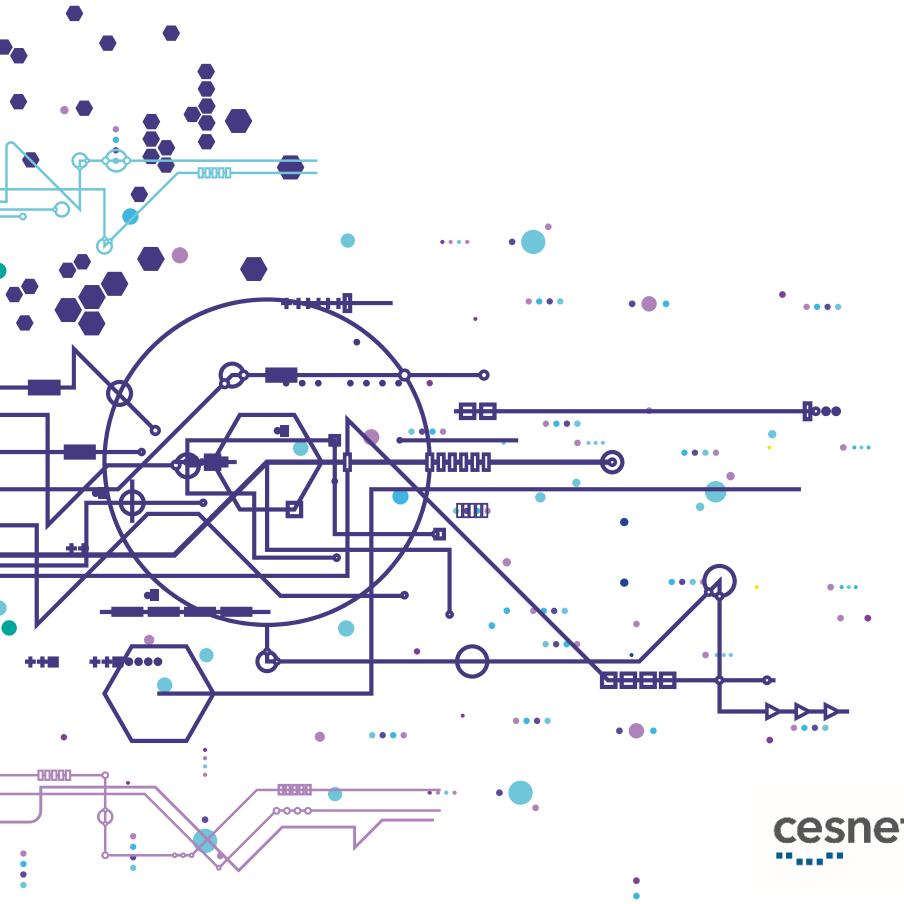
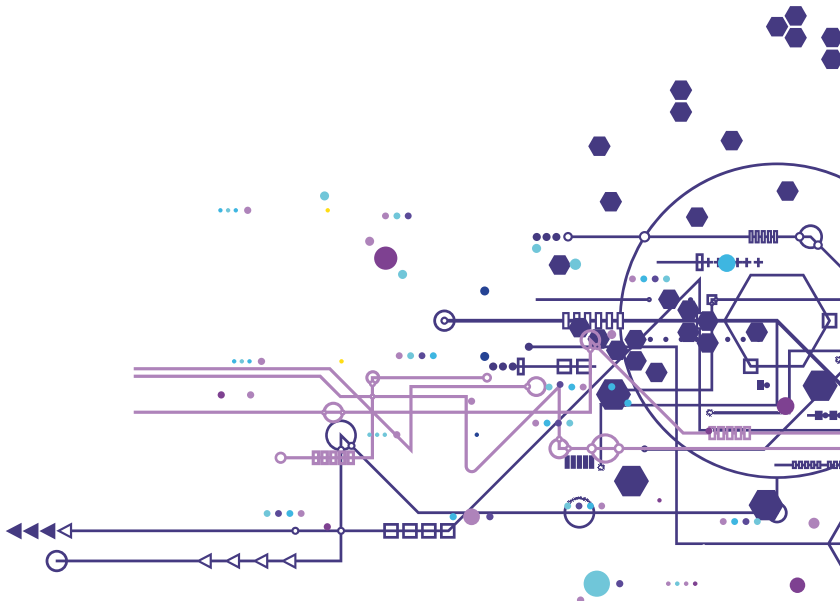
SECURITY

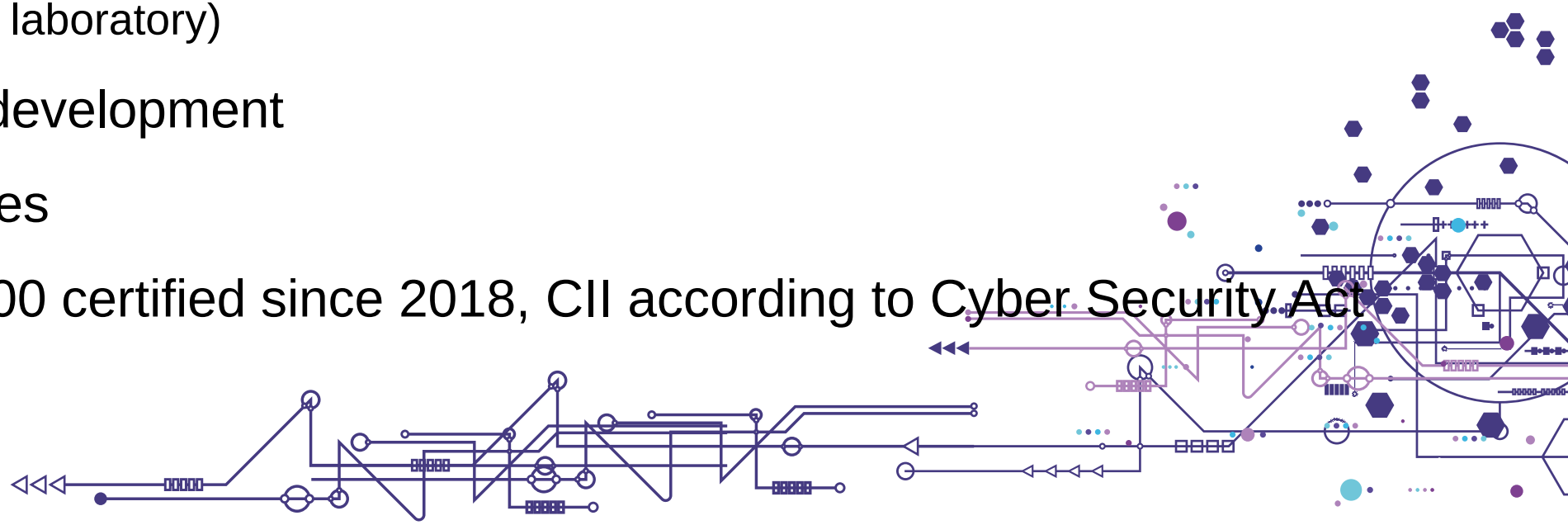
Andrea Kropáčová
andrea@cesnet.cz





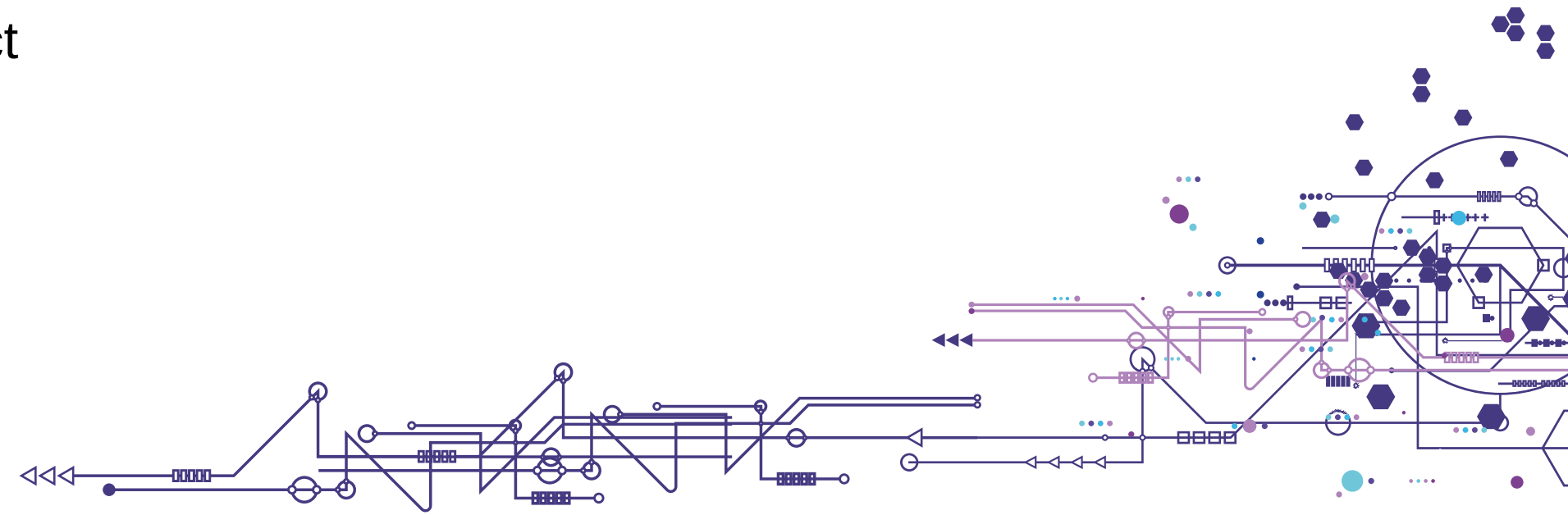
Introduction

- Security is one of our priorities
- Small but very efficient teams
  - Monitoring and defense
  - Security team CESNET-CERTS
  - FLAB (Forensic laboratory)
- Security tools development
- Security services
- ISMS, ISO27000 certified since 2018, CII according to Cyber Security Act

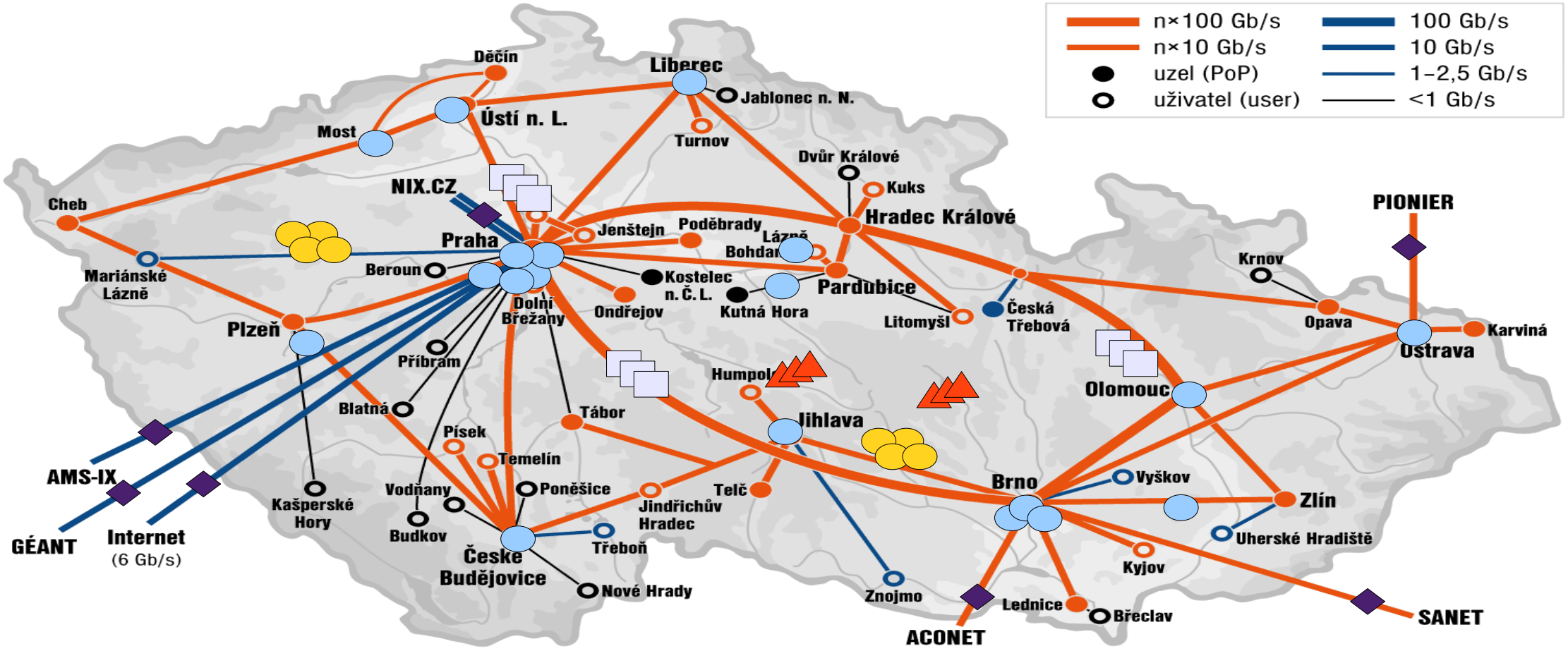


Our mission

- Keep the network running
- Keep services running
- To ensure safe access to our services
- To ensure the availability, confidentiality and integrity of data
- You can expect
  - Protection
  - Help
  - Cooperation



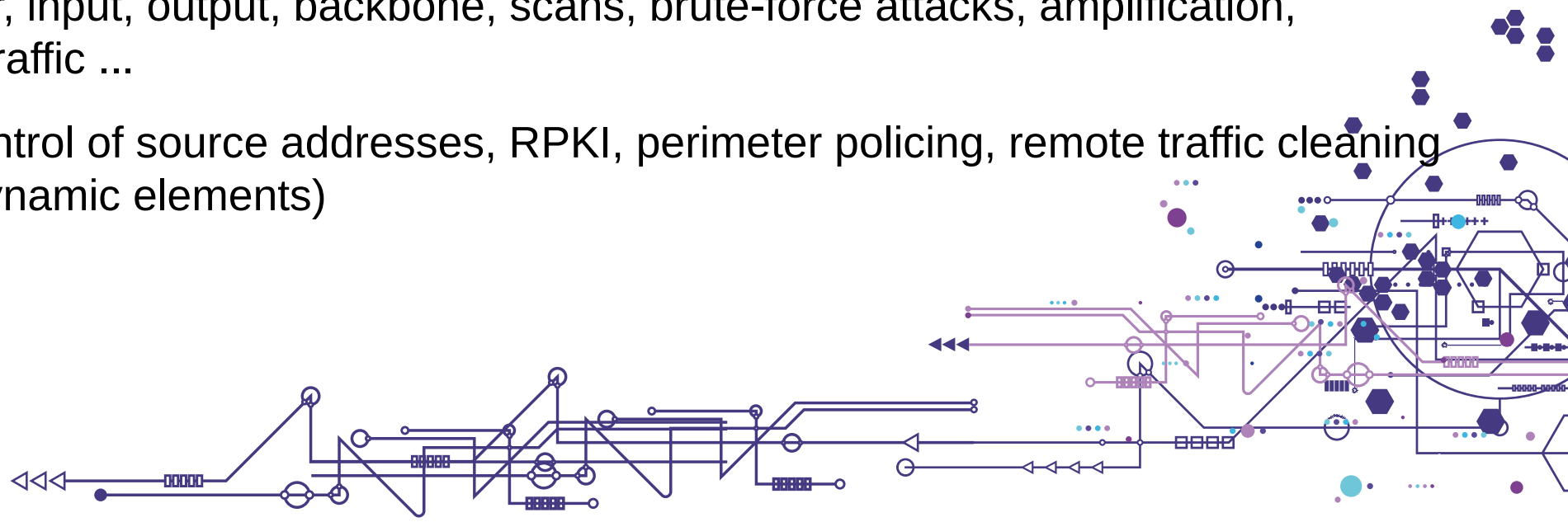
Security monitoring



- HW accelerated probes
- large scale (backbone-wide) flow based monitoring (NetFlow data sources)
- Honey Pots
- IDS, IPS, tar pit based systems, etc..
- SNMP based monitoring

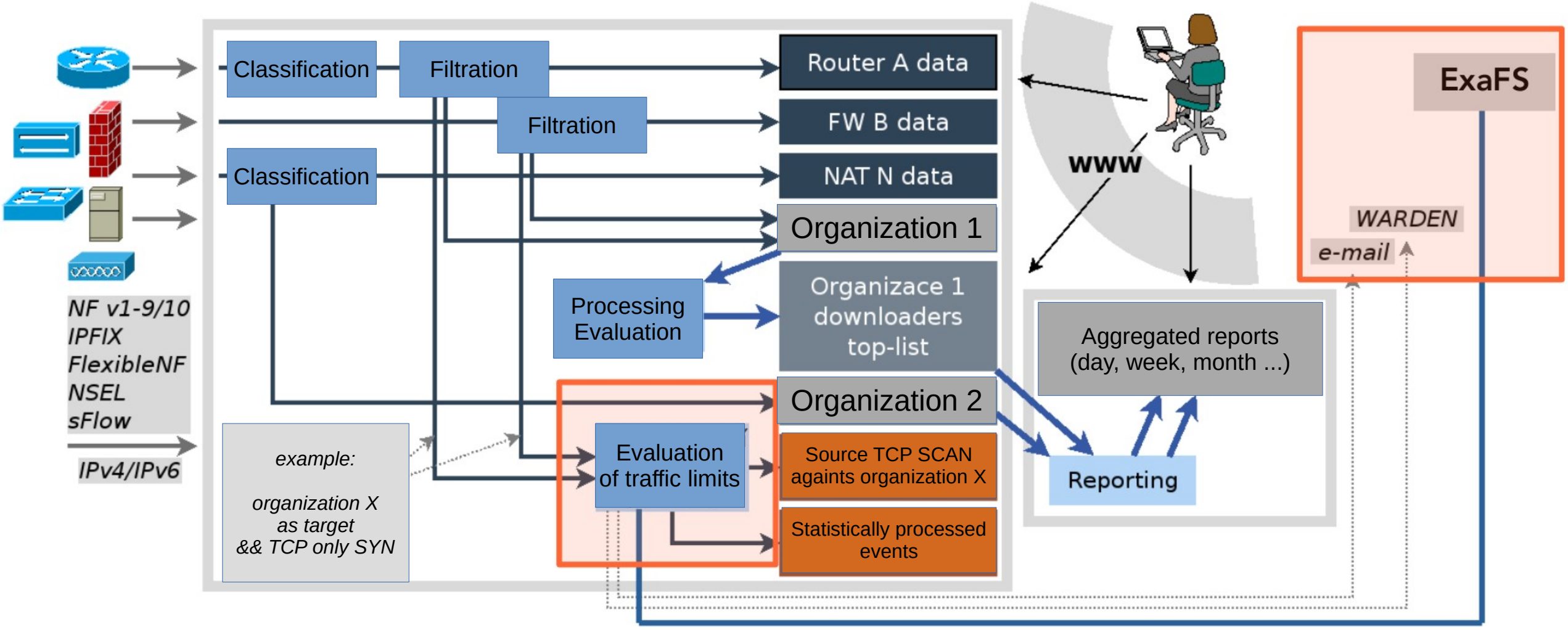
Monitoring and defense

- Based on FTAS and exaFS
  - detection and treatment of illegitimate traffic
  - to avoid congestion of backbone
  - no limits on legitimate traffic
  - m & m: perimetr, input, output, backbone, scans, brute-force attacks, amplification, anomally data traffic ...
  - access lists, control of source addresses, RPKI, perimeter policing, remote traffic cleaning ... (static and dynamic elements)



Traffic monitoring by FTAS

- Processing and evaluation process

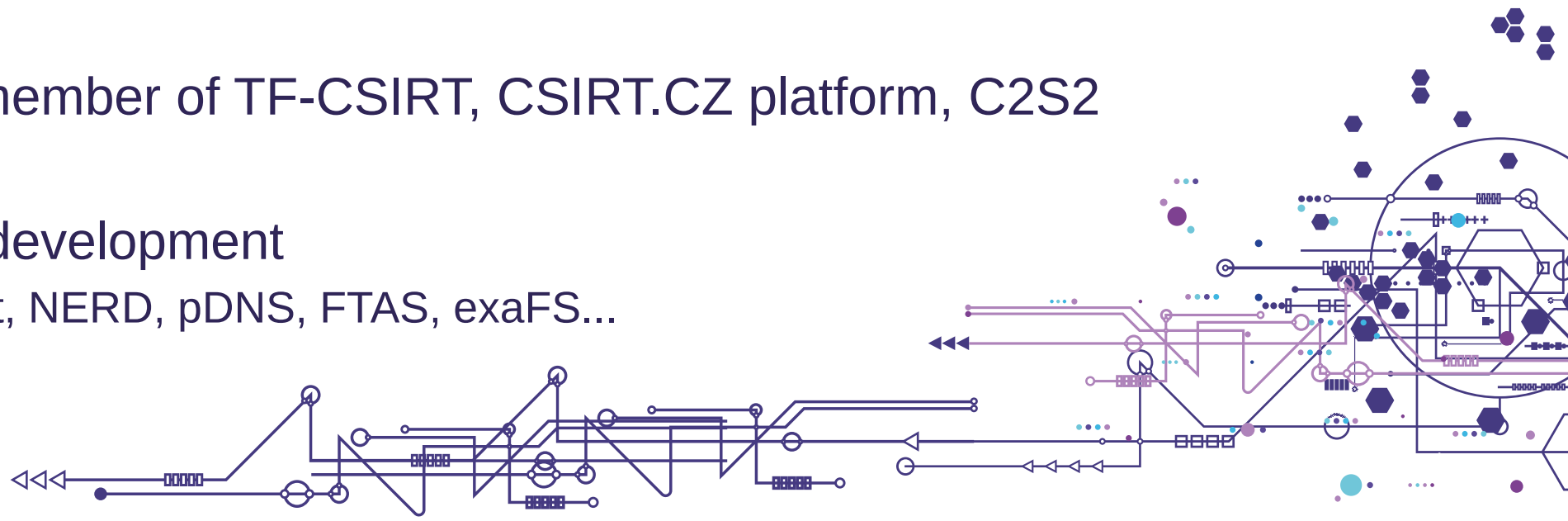


CESNET-CERTS

- Since 2004
- Accredited by Trusted Introducer
- 10 members (but not full time)
- Incident handling/response for the entire CESNET infrastructure (AS2852)
- csirt.cesnet.cz, abuse@cesnet.cz

- Cooperation: member of TF-CSIRT, CSIRT.CZ platform, C2S2

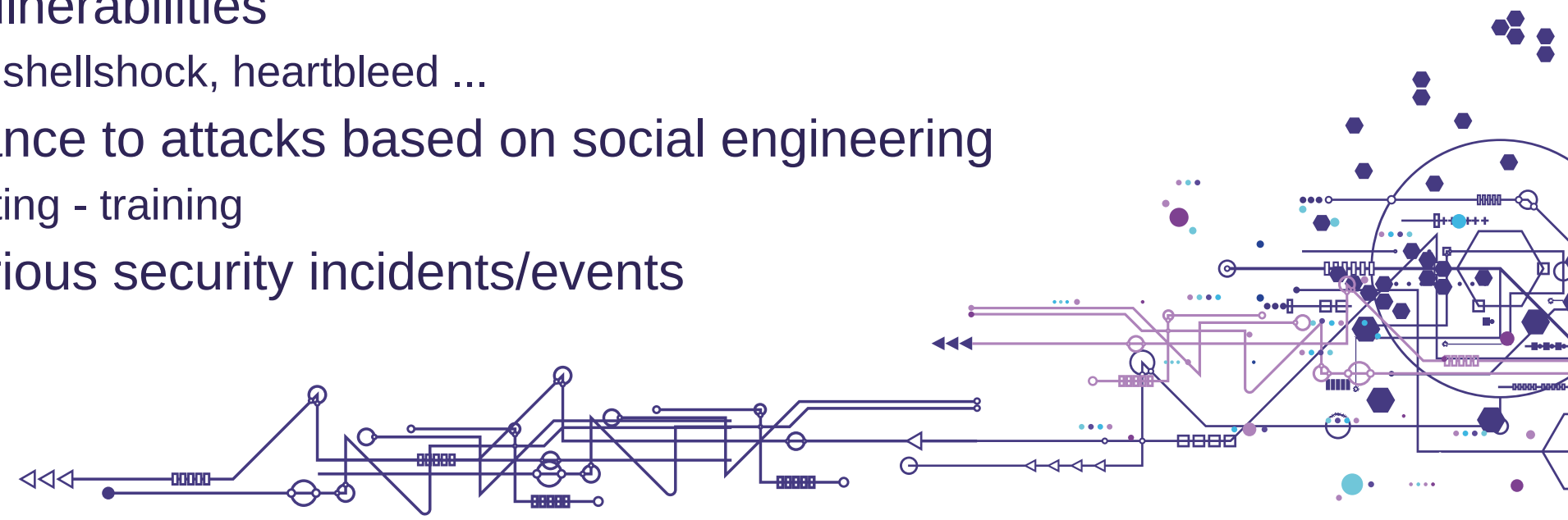
- Security tools development
  - Warden, Mentat, NERD, pDNS, FTAS, exaFS...



FLAB (Forensic laboratory)

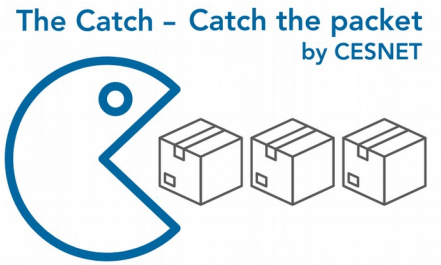
- Special unite, since 2011

- Penetration testing
  - network infrastructure, AAI infra, key services ...
  - on regular basis
- Tests for for vulnerabilities
  - memcached, shellshock, heartbleed ...
- Test for resistance to attacks based on social engineering
  - training – testing - training
- Analysis of serious security incidents/events
- Stress tests



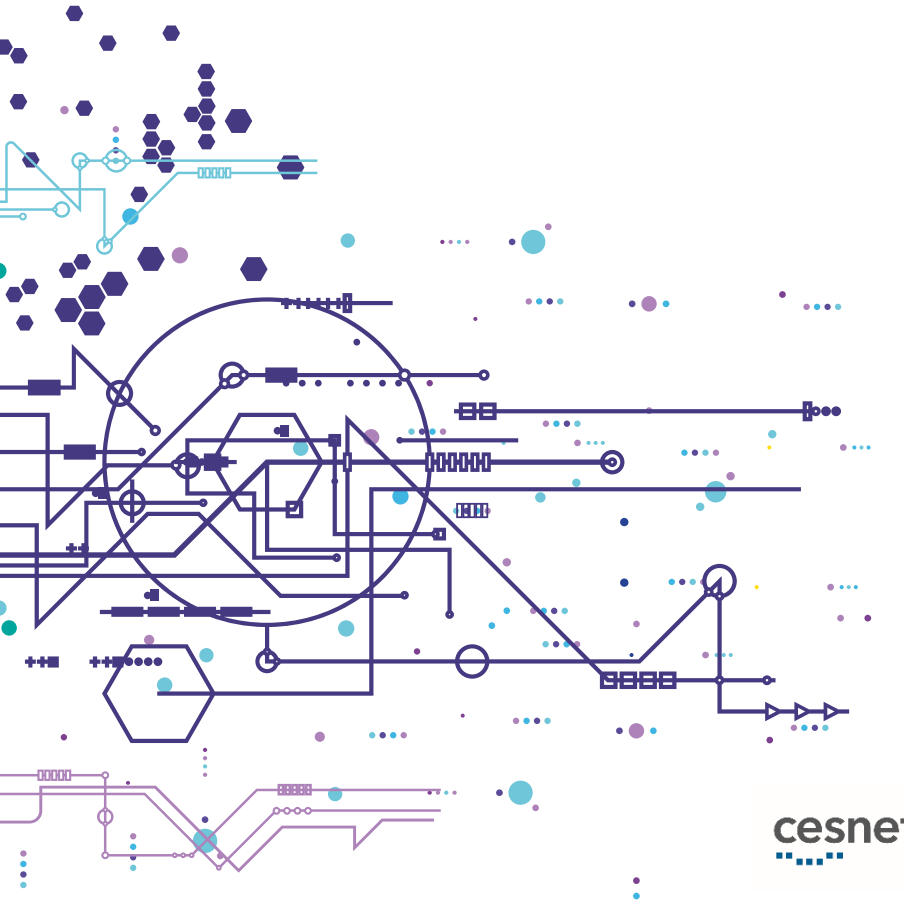
Other activities ...

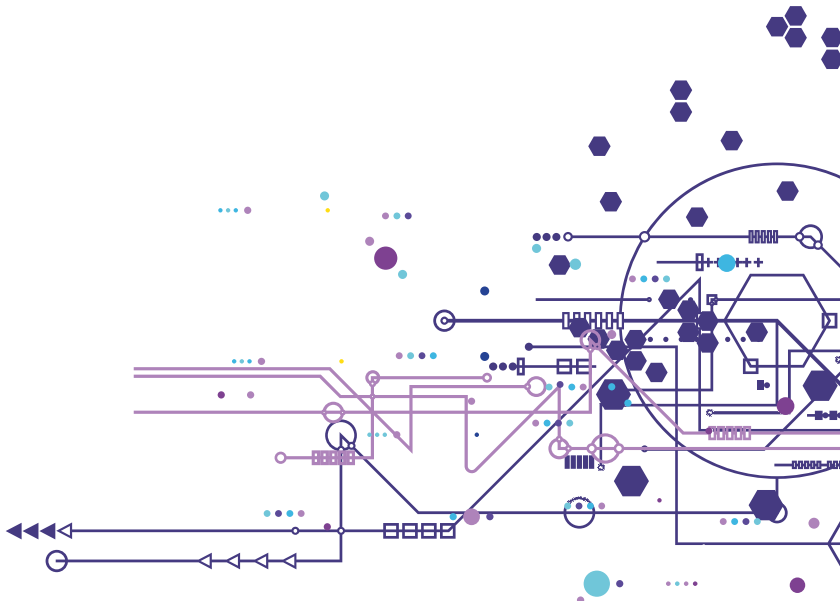
- Security Conference
  - every year, usually in Feb
  - 7 Feb 2023
- Workshops
  - security event processing, secure network design, FTAS as a service
- The Catch
  - our contribution to Cyber Security Month
  - https://www.thecatch.cz
- csirt-forum@cesnet.cz
  - mailing list, send mail to *csirt-forum-subscribe@cesnet.cz*
  - info about events, situational awareness
- Trainings
  - FT1, FT2
  - https://flab.cesnet.cz/cs/sluzby/skoleni
-



Thank you for your attention

Andrea Kropáčová
andrea@cesnet.cz





Napište nám

info@e-infra.cz