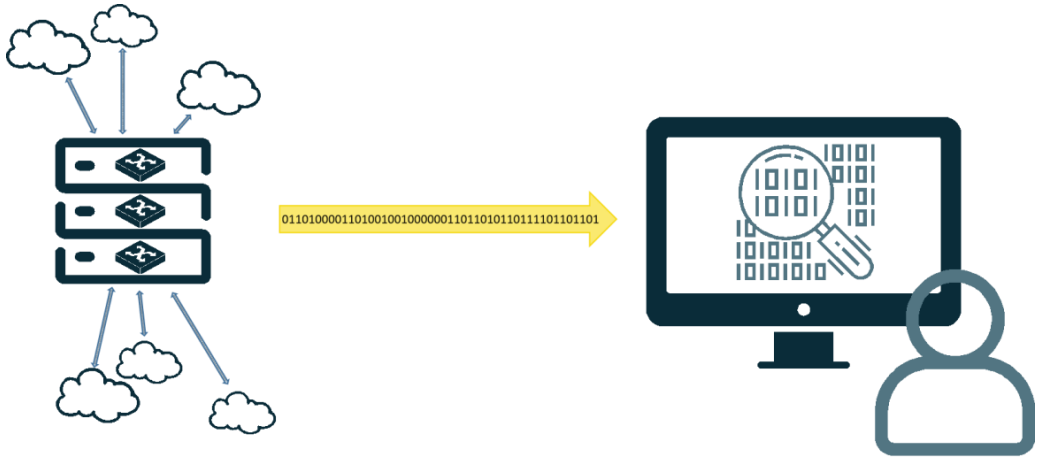
IPFIX Export at IXPs

Daniel Wagner – May 17th 2021

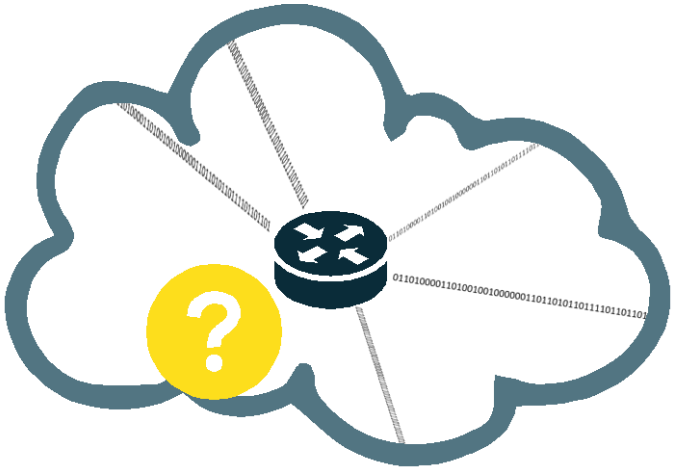
Introduction

- About me:
  Daniel Wagner
  Member of research group at DE-CIX
- About the product:
  Free service for customers to receive their IPFIX subset



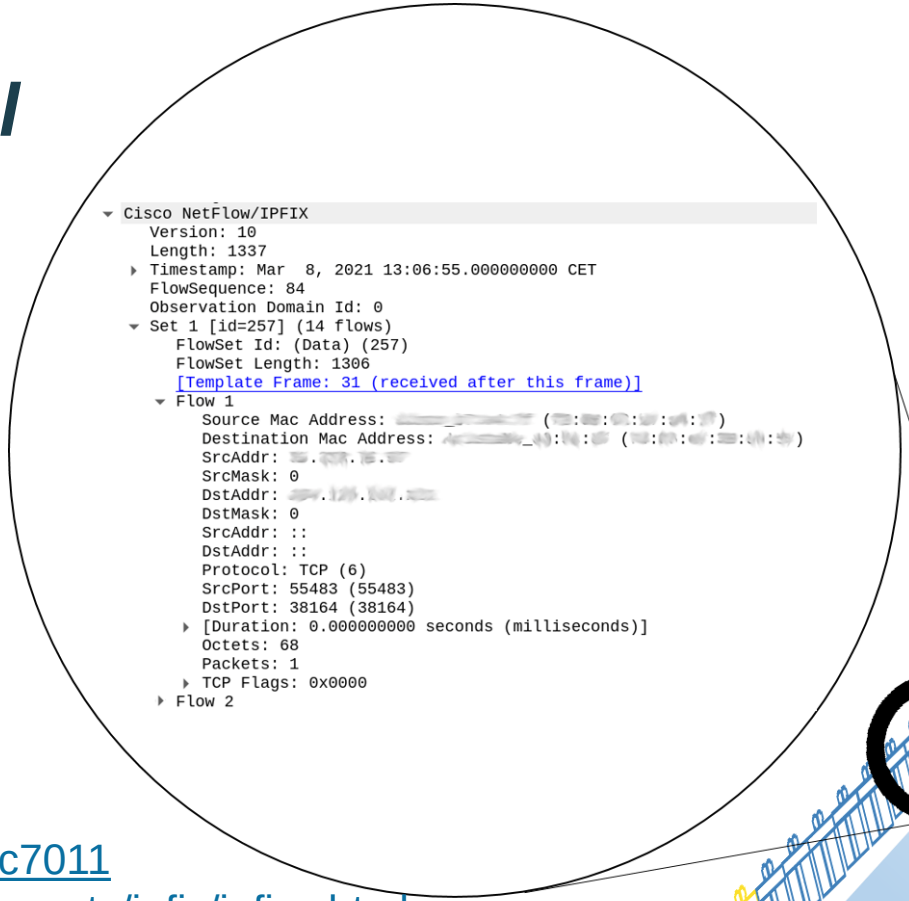
Motivation

- ➔ Insights in traffic statistics
- ➔ Beyond customer‘s rate limit
- ➔ No load on customer‘s router
- ➔ No router configuration needed



IPFIX Protocol

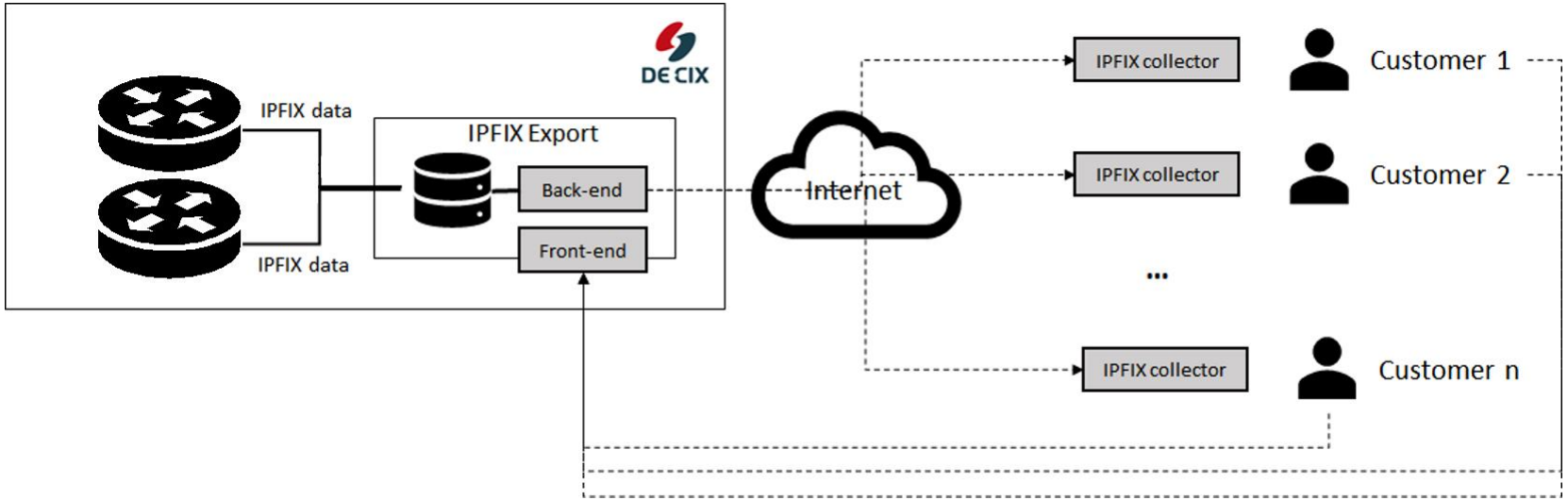
- RFC7011[1]
- Templates
- 491 data fields defined[2]
- Dead and alive timeout



[1] https://tools.ietf.org/html/rfc7011
[2] http://www.iana.org/assignments/ipfix/ipfix.xhtml

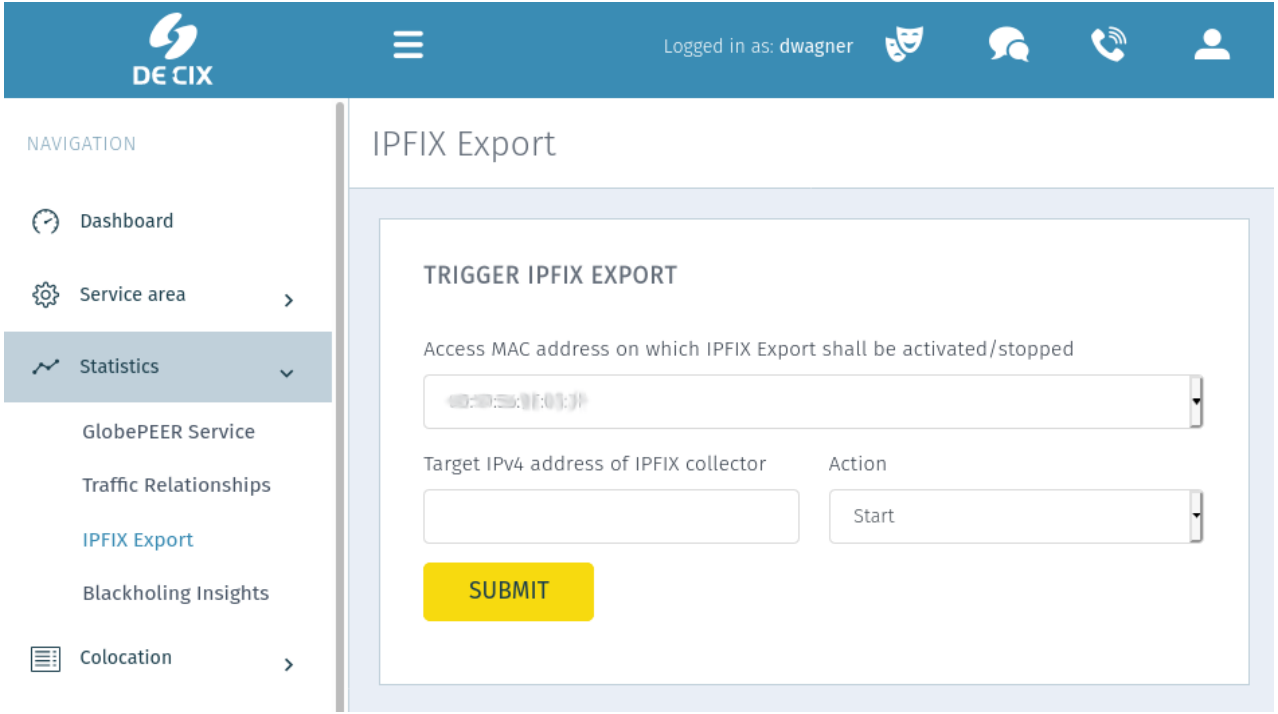
Architecture

- Packet sampling rate 1:10k
- Dead timeout: 15s, alive timeout 60s



Front-End[3]

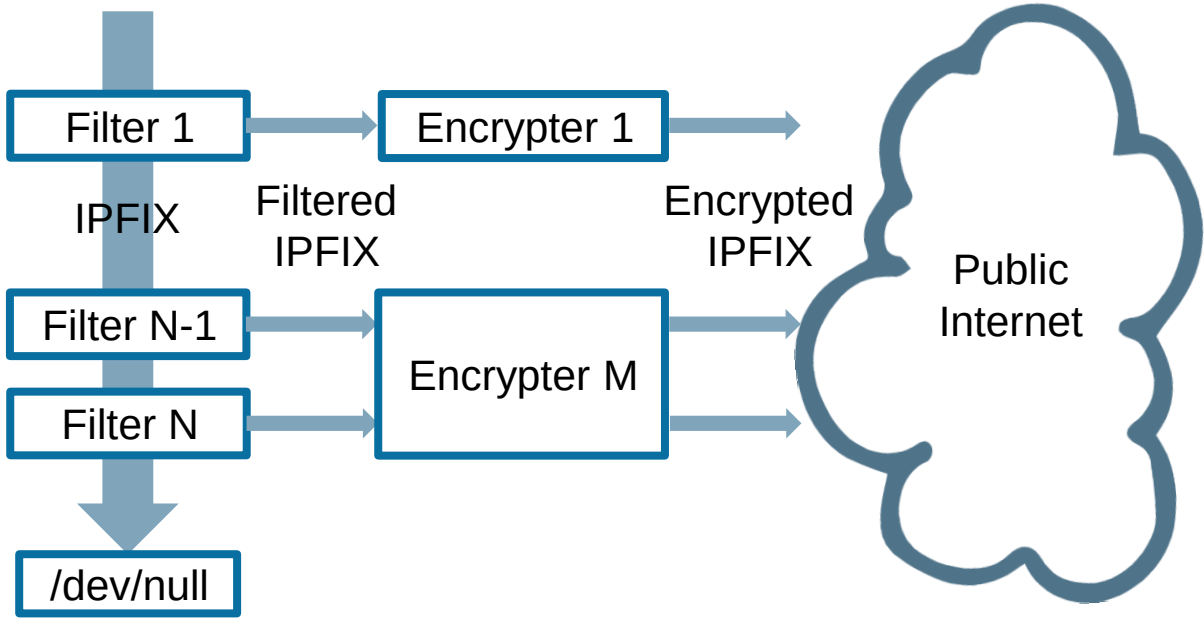
- Customers choose from their MAC addresses
- Enter any target IP
- Select start/stop



[3] https://portal.de-cix.net/statistics/ipfix-export

Implementation Challenges

- Incoming:
  One large IPFIX stream
- Outgoing:
  N filtered IPFIX streams to M target IP addresses
- Need for new IPFIX stream creation



Design Space

- **All-config, 1 Vermont[4] instance**
  - Config contains filters for every MAC address
  - Output redirected to encrypter on demand
- **„Config-on-demand“, 1 Vermont instance**
  - Config updated on demand
- **„Full-dynamic“, N Vermont instances**

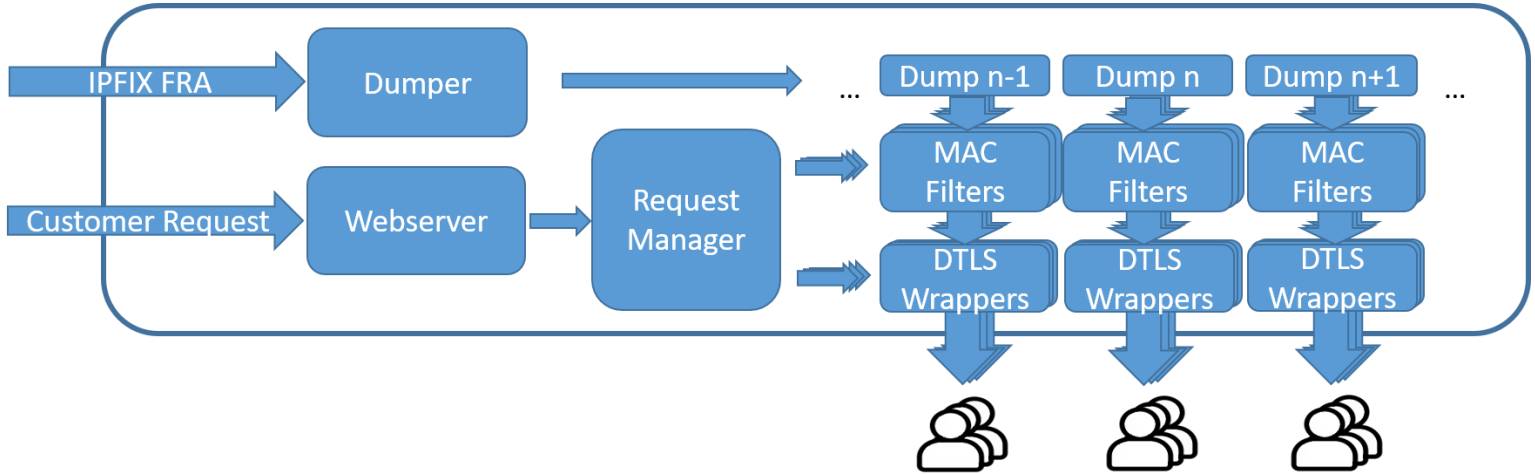
[4] https://github.com/tumi8/vermont/

Design Decision

	Interruption due to MAC change	Interruption due to export request	Efficiency	Export delay	Export chunking	Cleanup necessary
All-config	Yes	No	Poor	None	None	No
Config on demand	No	Yes	Good	None	None	No
Full dynamic	No	No	Good	~1 min	Yes	Yes

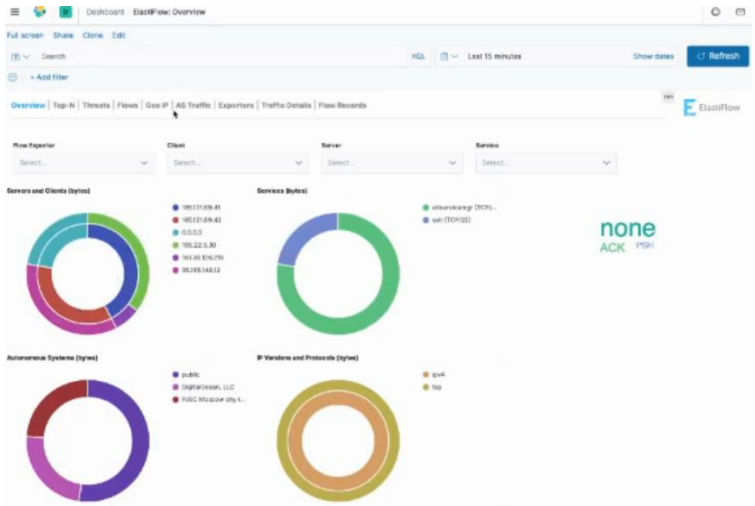
Back-End

- → Dumping + filtering: Vermont
- → No interruption upon request
- → Approx. 1 minute delay



Receiving Data

- Open-source decrypter[5]
- Pmacct[6]
- FastNetMon[7]

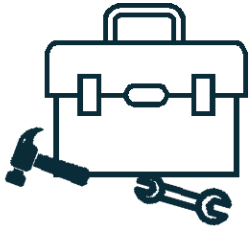



```
[dwagner@ ~]$ ./dtls-decrypter --listen :2055
--output 127.0.0.1:2055
Listening on :2055 (UDP) for DTLS traffic.
Sending decrypted traffic to 127.0.0.1:2055 (UDP)
Packets received: 1368  Bytes received: 335847
```

[5] https://github.com/de-cix/udp-dtls-wrapper/
[6] http://www.pmacct.net/
[7] https://fastnetmon.com/

Planned Enhancements

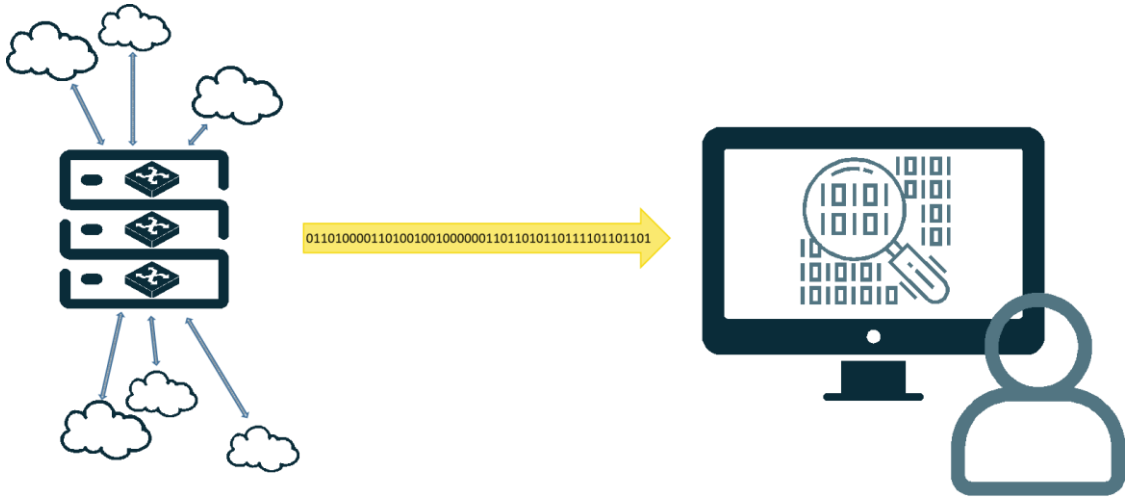
- ➔ Configure transport port
- ➔ Overview of running exports
- ➔ Export via IPv6
- ➔ Support other DE-CIX sites
- ➔ Webinar [8]

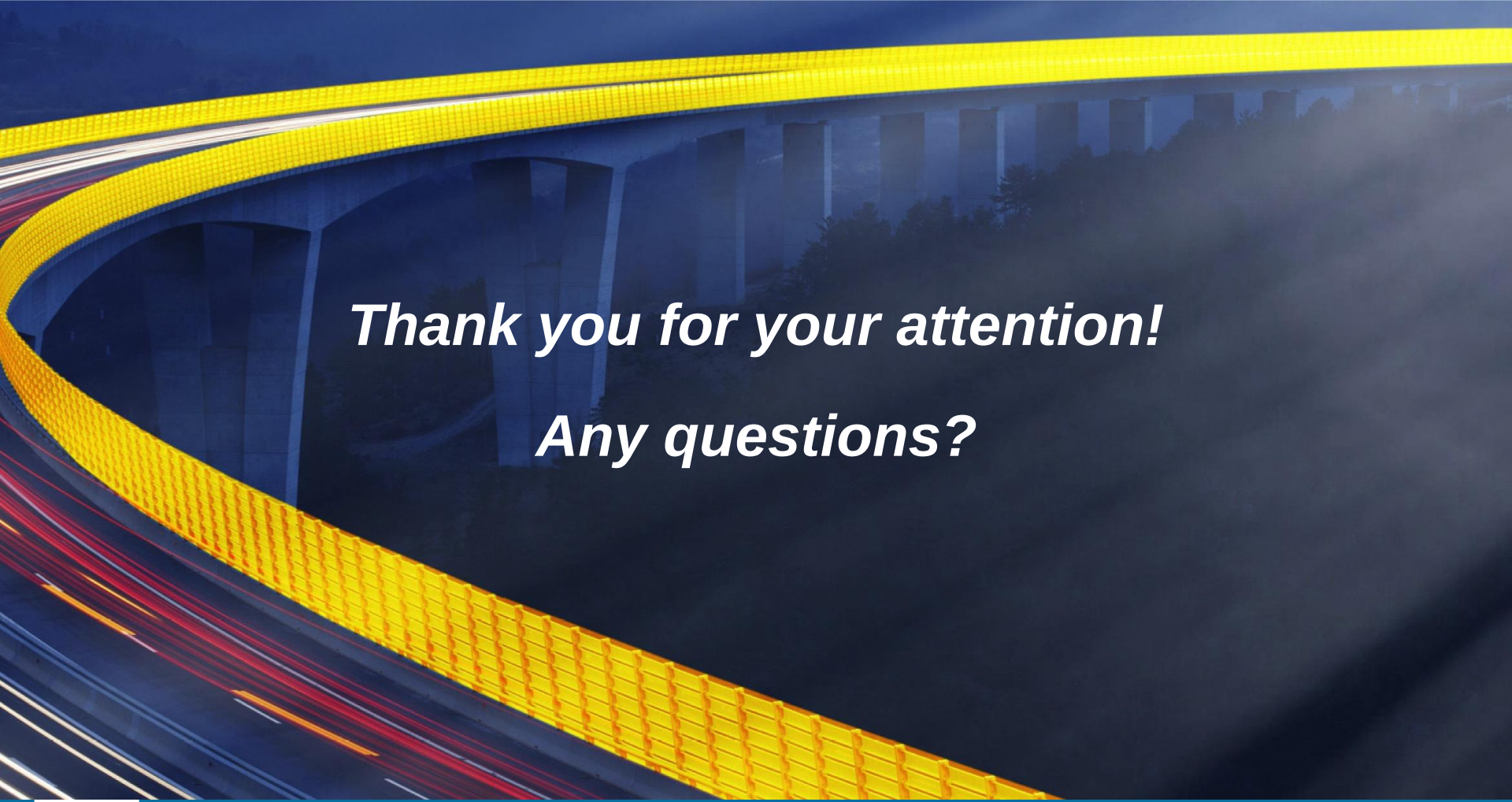


[8] https://www.de-cix.net/de/about-de-cix/academy

Summary

- Self-Managed IPFIX collection
- Sensible data encrypted
- Analysis with own tools
- Free beta service




Thank you for your attention!
Any questions?