Panel discussion:
Alert sharing and analysis – how to promote alert sharing and advance the analysis

Panelists

- Alexandre Dulanoy (CIRCL)
- Aaron Kaplan (CERT-AT)
- Piotr Kiejewski (CERT-Polska)
- Pavel Kácha (CESNET-CERTS)
- Jan Vykopal (CSIRT-MU)
- Robert Šefr (CSIRT-CZ)
- You

- Martin Žádník (CESNET)

Story 1

- Organizations in Czech NREN share security events
- Selected and aggregated events are redistributed to interested organizations
- NREN serves as a network honeypot for other service and network providers in national cyberspace
- Goal is to spread such a honeypot accross national cyberspace as well as mine and utilize shared events to protect cooperating networks

Story 2

- CZ.NIC

- Project Turris as a nation-wide honeypot producing lot of primary data
- CSIRT.CZ is aggregating vast number of event feeds (through IntelMQ) and distributing reports to its constituency

- Goal is to deliver quality events only (relevance, timeliness, accuracy, completeness and ingestibility)

Topic

- Let’s skip legal boundaries within EU and national legislation

- Let’s discuss content challenges
  - Data related issues such as (detail of shared information, quality of shared information, false positives, ...)
  - Missing elements in existing systems
  - Barriers in sharing, motivation

Question 1

How do you deal with possibly low quality of data (false positives, late arrival, irrelevant data, cycles)?

Question 2

Do you feel that your partners can easily connect data producers?

Question 3

Is it possible to backtrack primary logs (packets, flows, IoC) which are the cause of shared events?

Question 4

What is the biggest lesson learned from developing and deploying alert sharing?

Thank you!