International Telecommunication Union

Geneva Centre for Security Sector Governance

MISP INFORMATION SHARING PLATFORM DEMO

Rimtautas Černiauskas

Cyber security consultant, system architect

2019.10.02

INFO SHARING BUILDING BLOCKS

- MANDATE (Legal framework)
- Incident detection and analysis capabilities
- Procedures and SOP
- Sharing platform

INFO SHARING MANDATE

- High level legal act or **MOU.**
- Allows to host information sharing platform.
- Defines owner and participants.
- Permits to process personal data for cyber security reasons.

INCIDENT DETECTION AND ANALYSIS

- Detection - consumes shared threat intelligence data
- Incident analysis produces new threat indicators
- Builds National threat landscape
- Builds National situation awareness

PROCEDURES AND SOP

- Incident SOP
- Post incident analysis SOP
- Incident classification and taxonomy
- Traffic Light Protocol for sensitive data protection

SHARING PLATFORM

- Integrated with international CERT community
- Available to national critical infrastructure owners
- Trusted and Secure
- Easy manageable multi organization environment

MISP PLATFORM

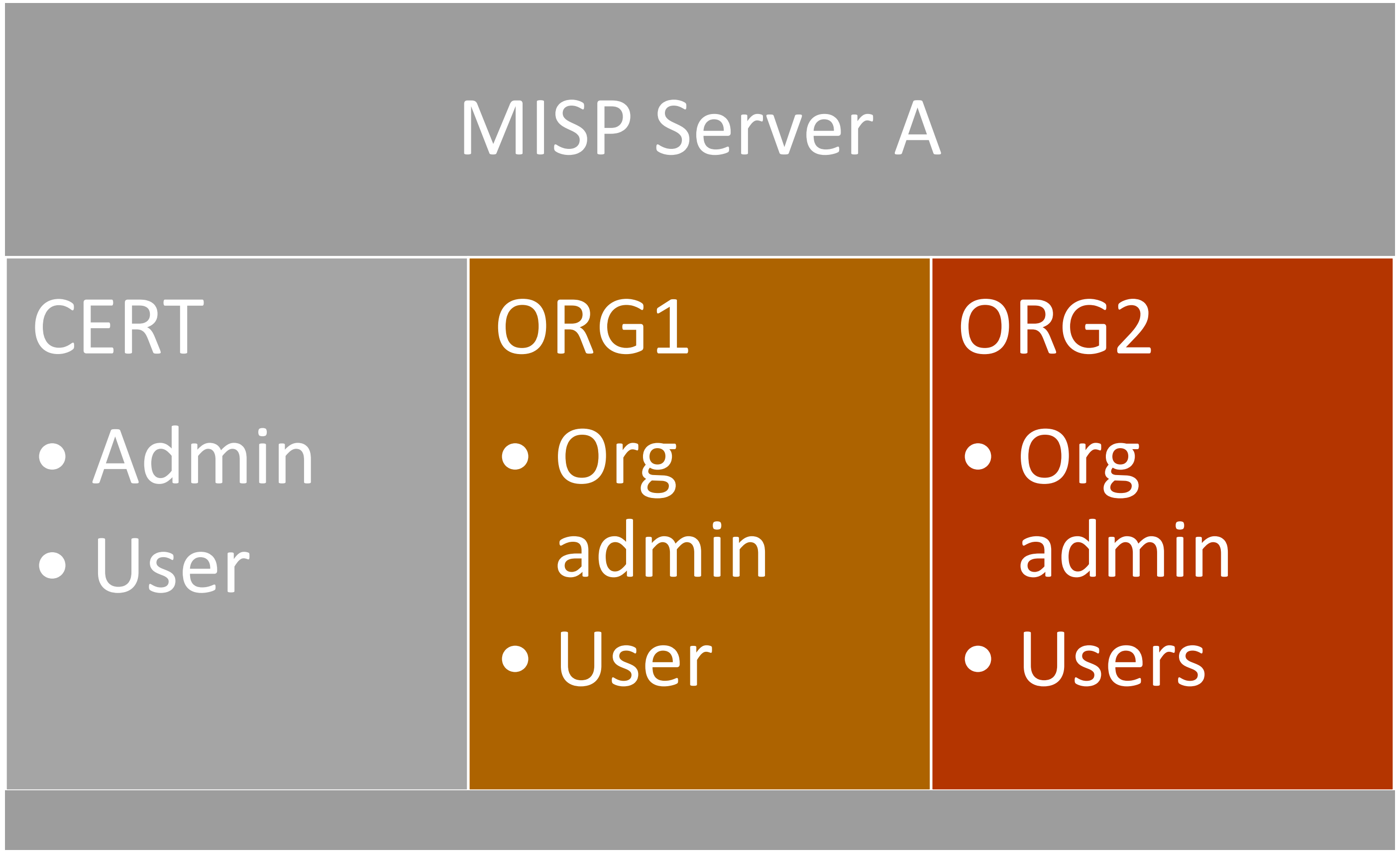
- Created by MOD CERT BE
- Developed by CERT LU and NATO
- Used by more than 2000 organizations worldwide
- Many different info sharing communities:
    - FIRST and Trusted Introducer
    - CIRCL MISP
    - NATO

MISP ORGANISATIONS AND USERS CONCEPT

- One main organization
  - Admin user to manage everything
  - Organization users with different rights

- More organizations
  - Org Admin
  - Org users

SINGLE MISP SERVER



MISP Server A

CERT

- Admin
- User

ORG1

- Org admin
- User

ORG2

- Org admin
- Users

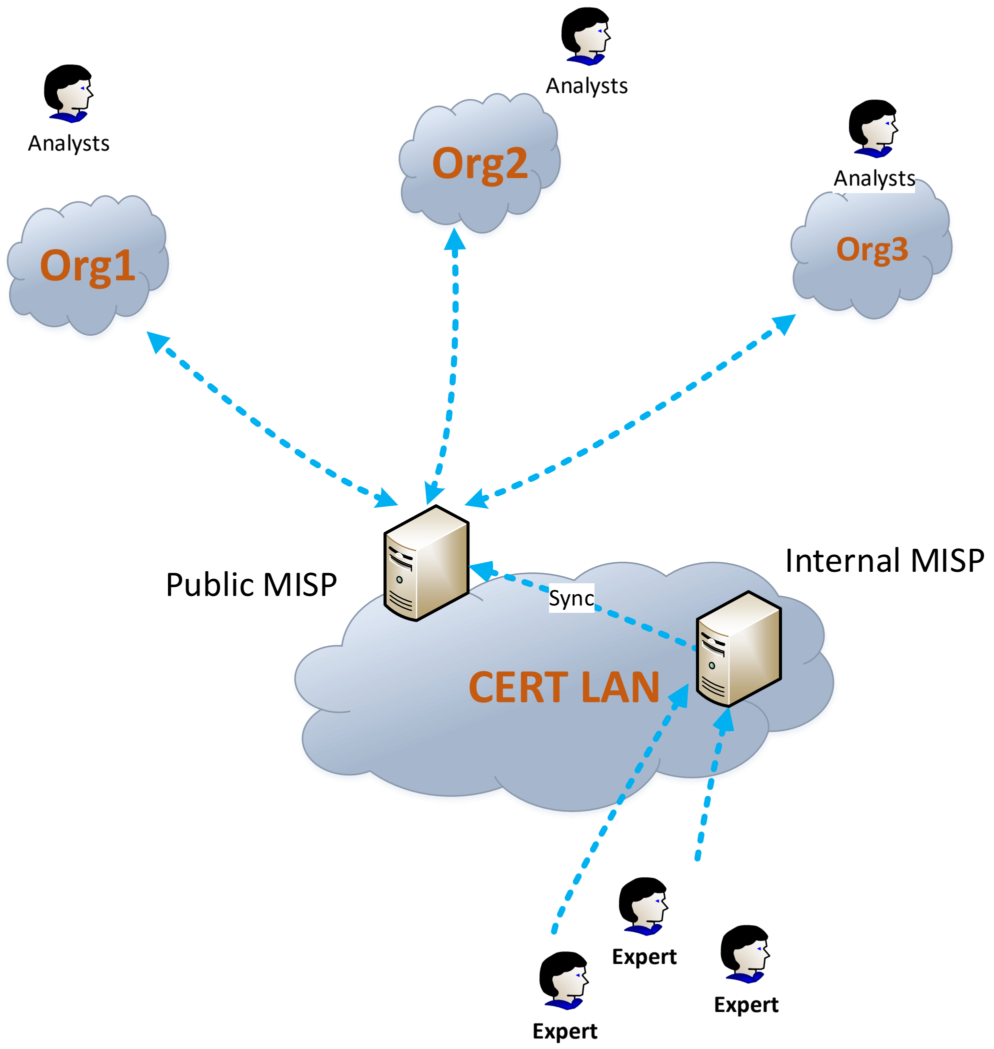
MISP COMMUNITIES

- Your organization only
- This community only
- Connected communities
- All communities

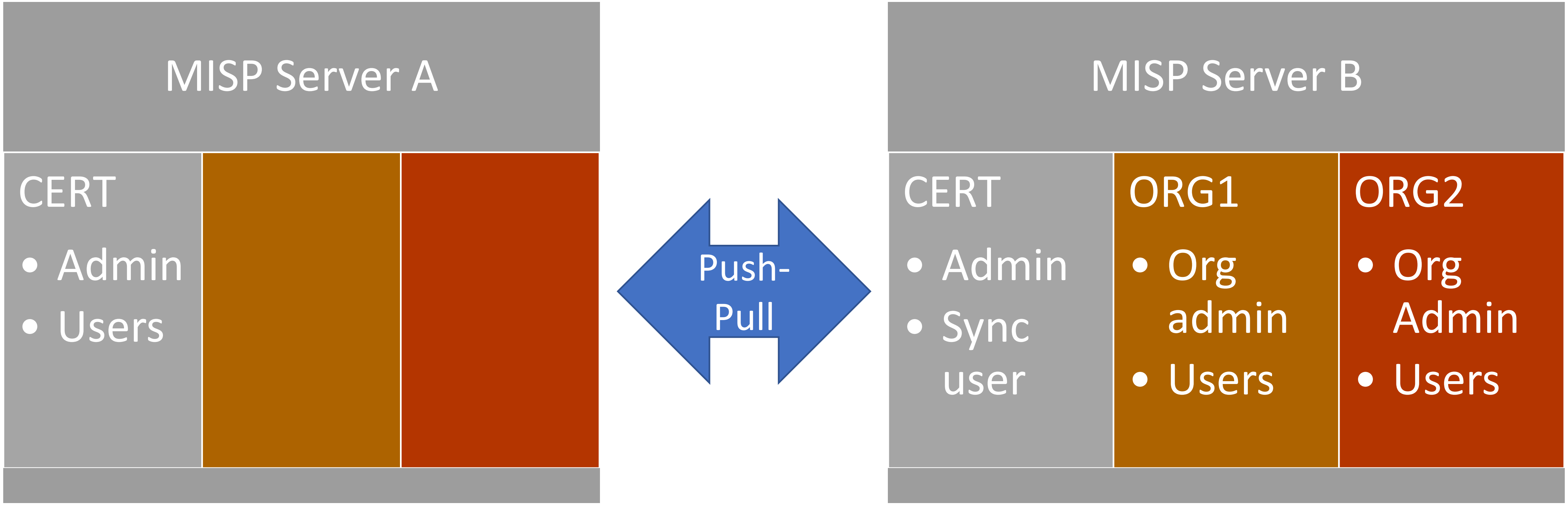
MISP INFORMATION SHARING DEMO1

- Local server case

PRACTICAL MISP IMPLEMENTATION



2 MISP SERVERS CONCEPT



MISP Server A

CERT

- Admin
- Users

Push-Pull

MISP Server B

CERT

- Admin
- Sync user

ORG1

- Org admin
- Users

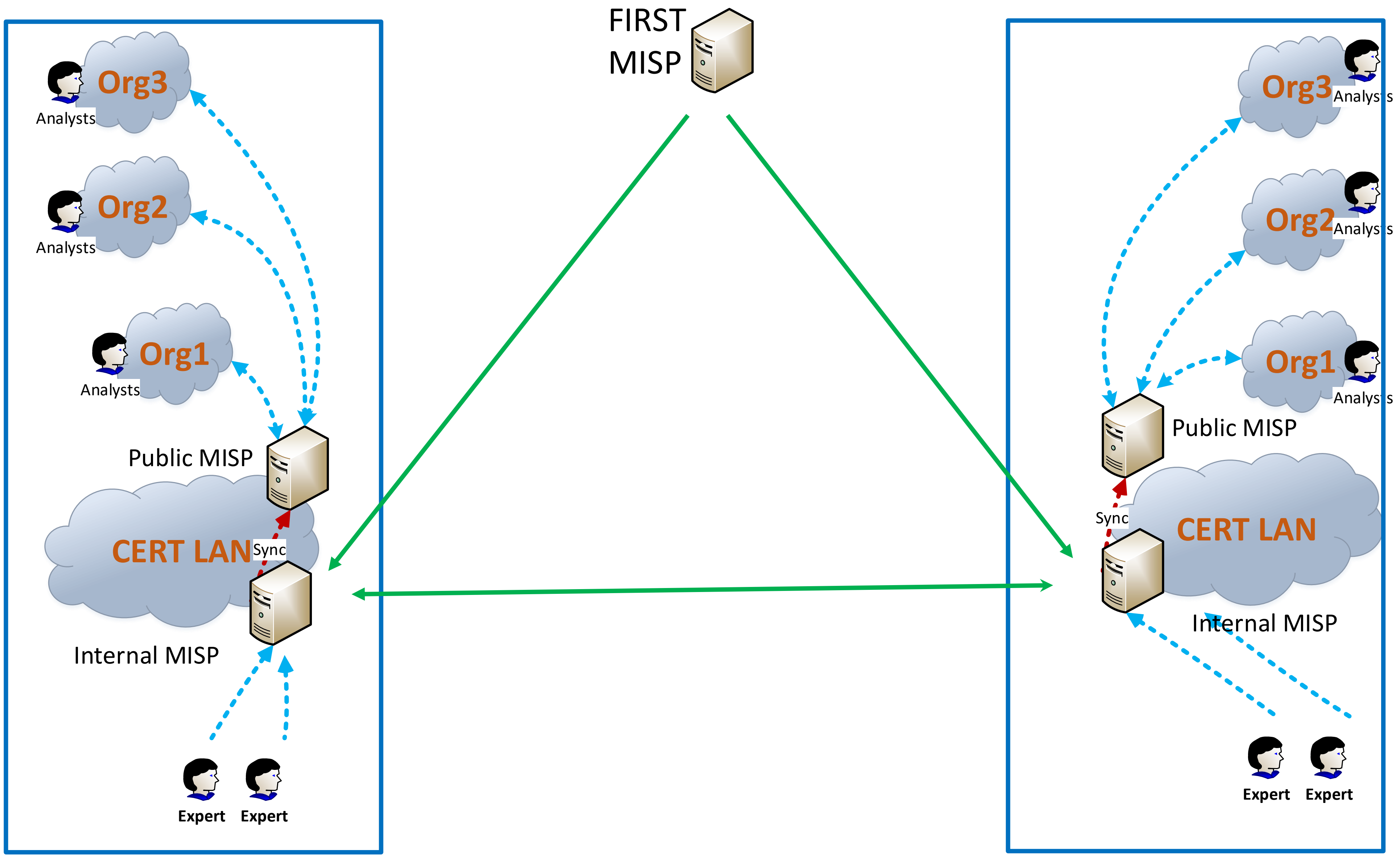
ORG2

- Org Admin
- Users

MISP INFORMATION SHARING DEMO2

- 2 server synchronization demo

INTERNATIONAL MISP



MISP INFORMATION SHARING DEMO3

- 3 server synchronization demo

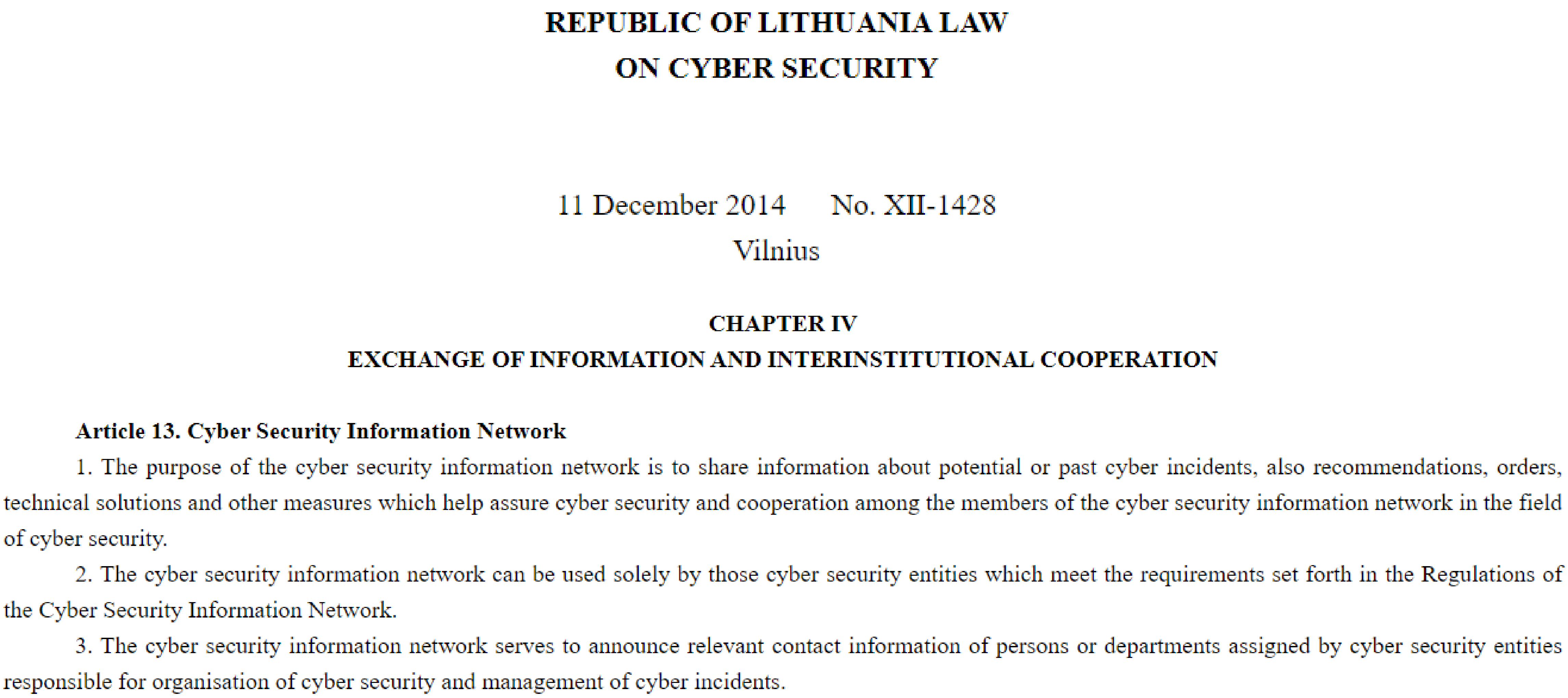
MISP SYNC FILTERS

- Organization filters
- Tag filters
- Different MISP instances
- Connected communities
- All communities

MISP INFORMATION SHARING DEMO4

- 2 server synchronization using filters demo

SHARING EXAMPLES



REPUBLIC OF LITHUANIA LAW
ON CYBER SECURITY

11 December 2014 No. XII-1428
Vilnius

CHAPTER IV
EXCHANGE OF INFORMATION AND INTERINSTITUTIONAL COOPERATION

Article 13. Cyber Security Information Network

1. The purpose of the cyber security information network is to share information about potential or past cyber incidents, also recommendations, orders, technical solutions and other measures which help assure cyber security and cooperation among the members of the cyber security information network in the field of cyber security.

2. The cyber security information network can be used solely by those cyber security entities which meet the requirements set forth in the Regulations of the Cyber Security Information Network.

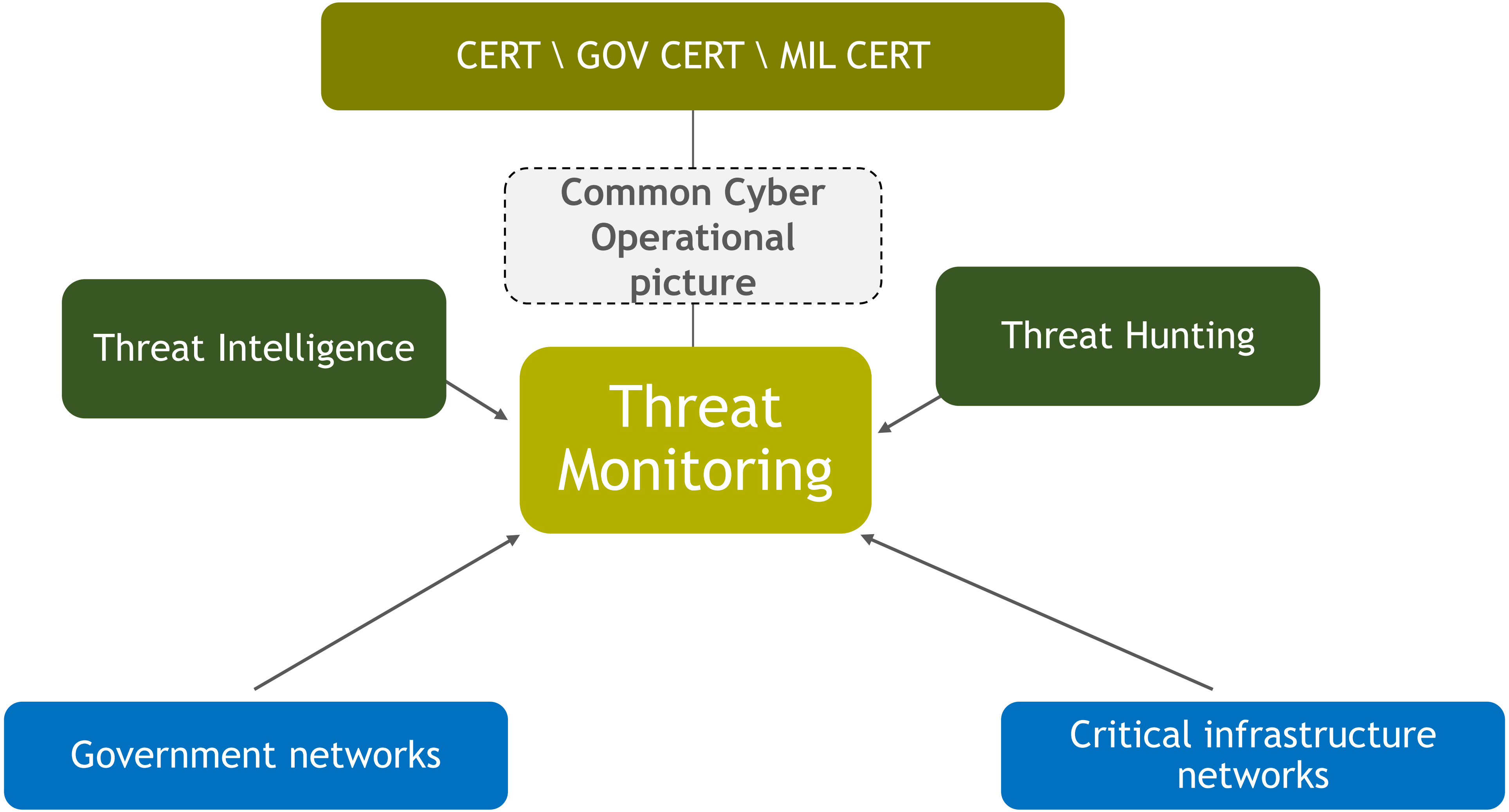
3. The cyber security information network serves to announce relevant contact information of persons or departments assigned by cyber security entities responsible for organisation of cyber security and management of cyber incidents.

SHARING EXAMPLES

2018 : S**ecurity Service of Ukraine, Antonov** sign memorandum on exchanging info about cyber-attacks in real time …. to secure a real-time exchange of technical information about cyber incidents between the two entities via the **MISP-UA** platform…

https://en.interfax.com.ua/news/economic/517302.html

Building Common Cyber Operational picture



CERT \ GOV CERT \ MIL CERT

Common Cyber Operational picture

Threat Intelligence

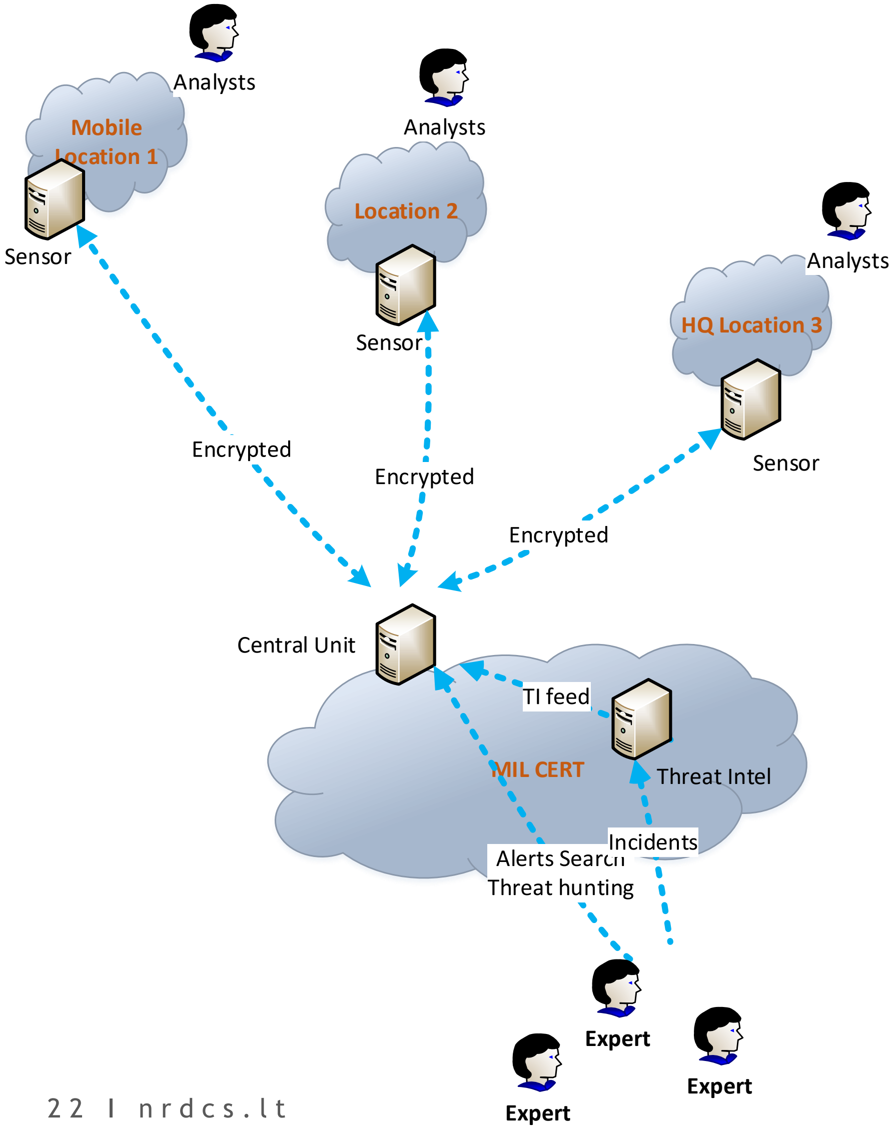
Threat Monitoring

Threat Hunting

Government networks

Critical infrastructure networks

SITUATION AWARNESS AT ALL LEVELS



CERT Experts

Full situation awareness across all networks:

1. Daily operations
2. CII situation monitoring
3. Both classified and unclassified networks
4. Static and deployable CIS

Local Analyst

Full visibility at local network level.

?

Rimtautas Černiauskas
rc@nrdcs.lt