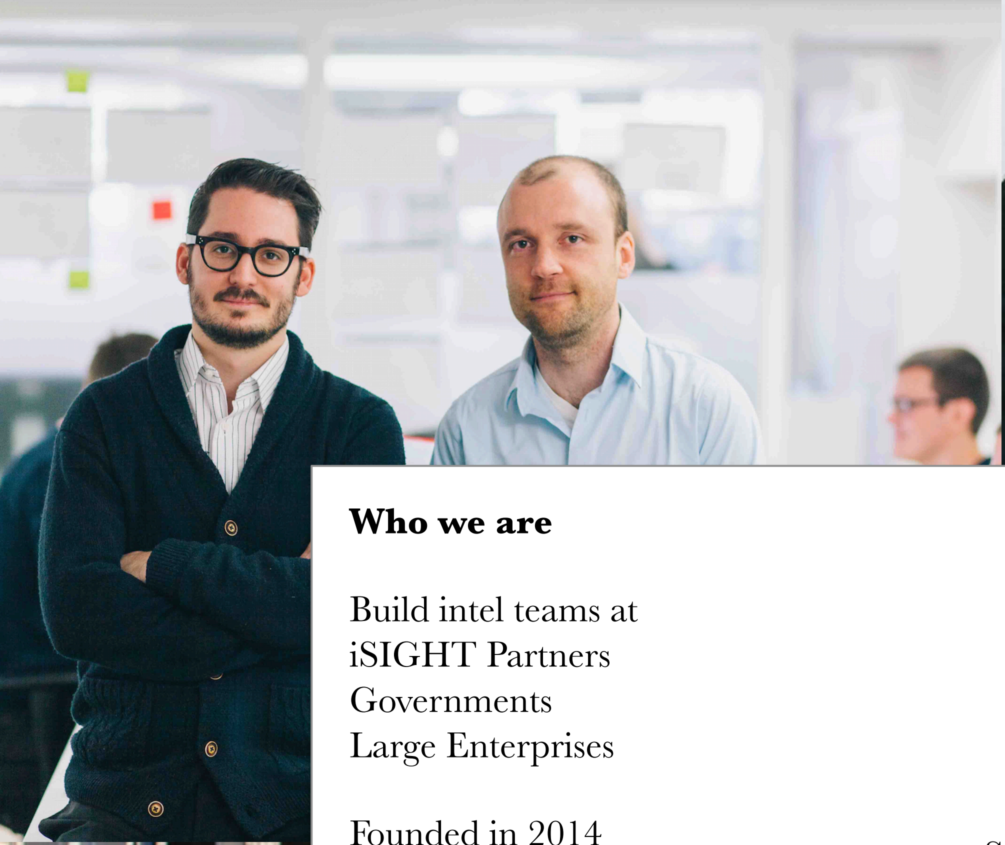
intelworks

ENISA WORKSHOP: THE FUTURE OF THREAT LANDSCAPE

Rapid innovation and ecosystem / complex system behavior in the threat landscape



Who we are

Build intel teams at
iSIGHT Partners
Governments
Large Enterprises

Founded in 2014
13FTE UX and Engineering

1.83M funding for 2015

What we’re building

TAXII Server (open-source)
TAXII Client (open-source)
STIX2JSON (open-source)
TAXII Directory (open)
STIX/TAXII Marketplace (open)

STIX/TAXII Platform (commercial)
exchange, ingest, enrich, consolidate -
analyst efficiency and workflow –
intel workflow and dissemination-

www.intelworks.com

FEEDBACK FROM INTELLIGENCE CAPABILITIES

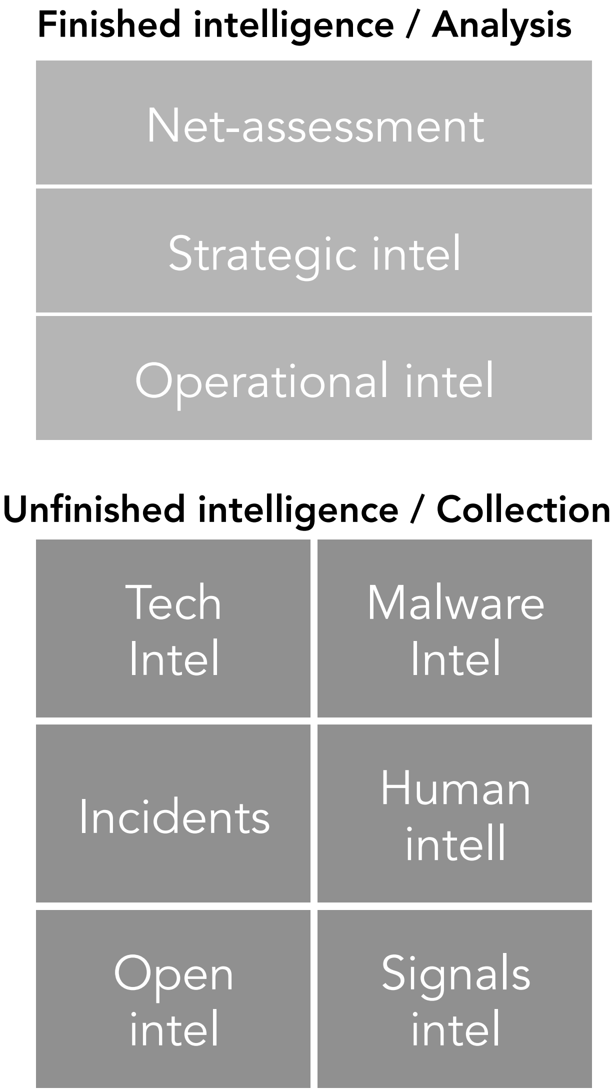
From:

13 intelligence suppliers, from
- The Netherlands
- Israel
- United States
- Russia
- Korea
- Pakistan

~10 intelligence capabilities in governments

Non-profit capabilities

Market analysts



Finished intelligence / Analysis

Net-assessment

Strategic intel

Operational intel

Unfinished intelligence / Collection

Tech Intel

Malware Intel

Incidents

Human intell

Open intel

Signals intel

TRENDS IN THREAT LANDSCAPE

- Rapid innovation and investment available, driving up cost of collection (vs analysis)

- Less re-use of compiled tools, infrastructure, decreasing value of indicators/observables

- Knowledge proliferation, also from cyber conflict to other problem areas, making certain problems more widespread or difficult to attribute

- More closed communities, increasing need for human and signals intelligence – other capability development

- Moving (back) to physical world

- **Overall:**
  "Network" / "Ecosystem" behavior

- Ecosystem means:
  Indicators -> Context -> Situational awareness

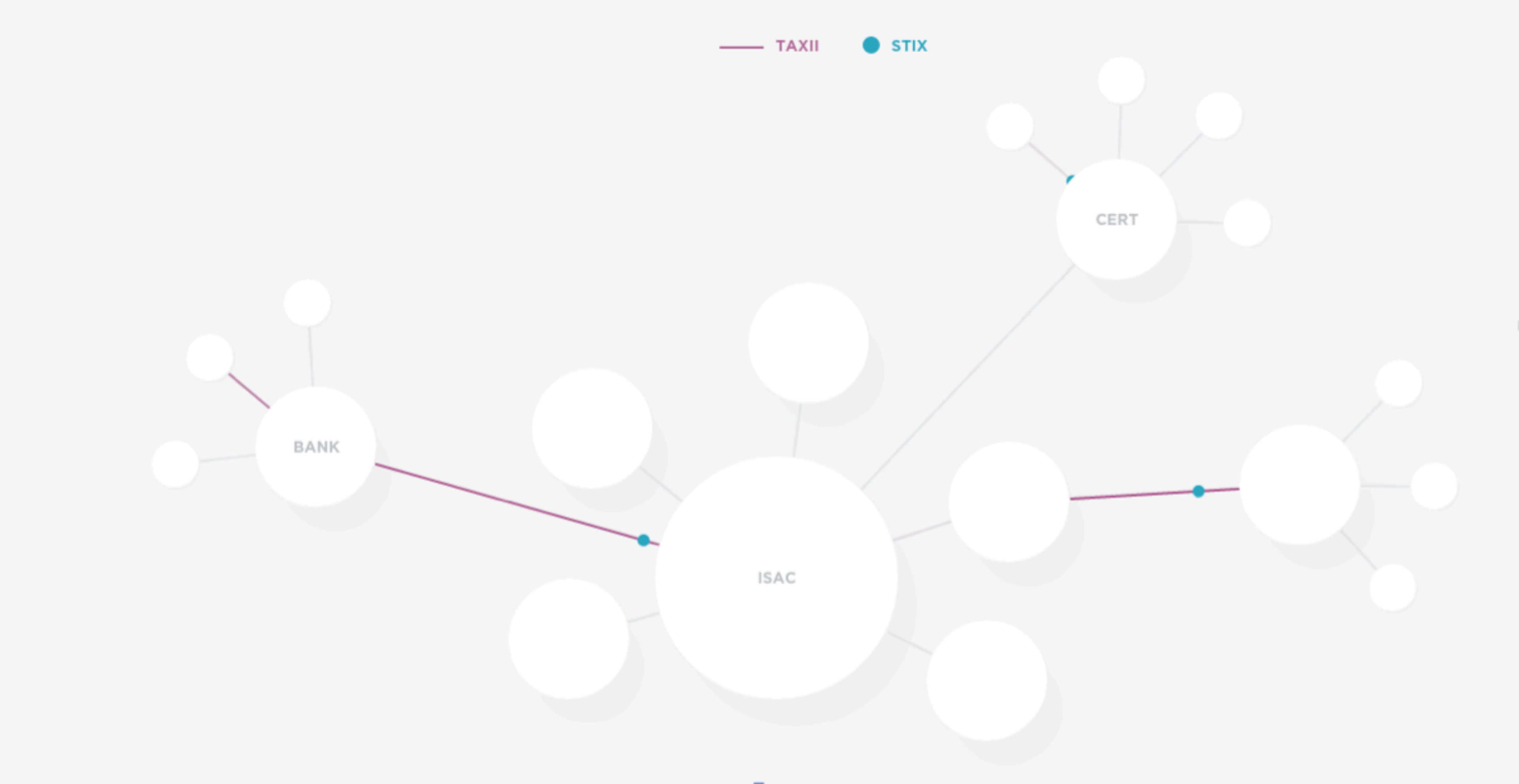
- Limited resources, large problem

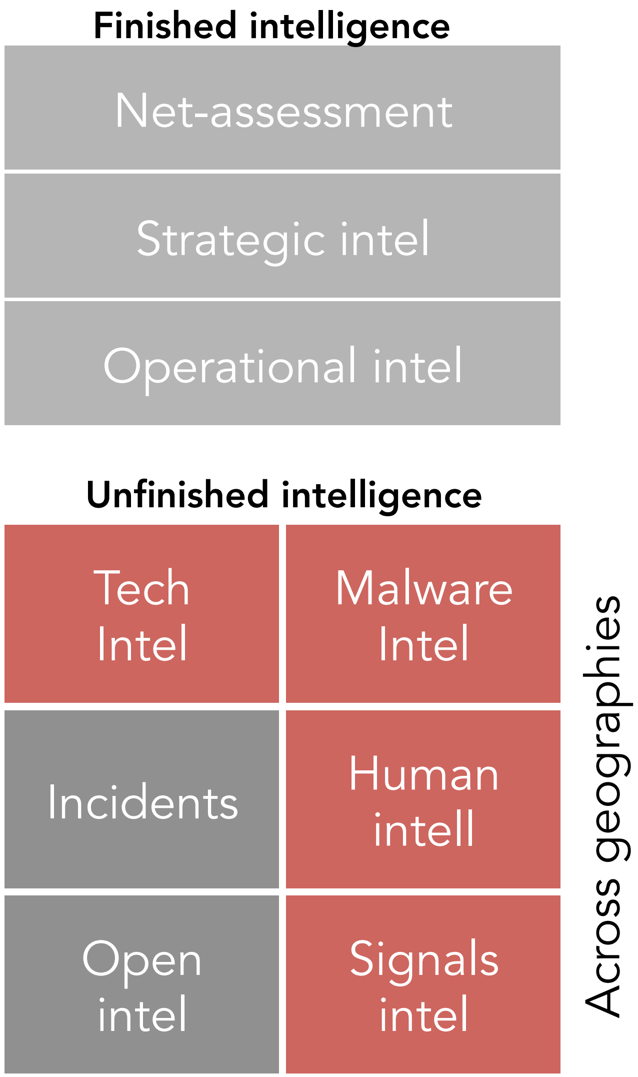
- Spend analyst time on relevant threats (alignment vs security)

- Ecosystem vs Ecosystem ("netwar")

BE AN "ECOSYSTEM": STIX/TAXII

- Unfinished intelligence exchange (large volume, low relevance, unfinished)
- Finished intelligence exchange (low volume, high relevance, finished)





Finished intelligence

Net-assessment

Strategic intel

Operational intel

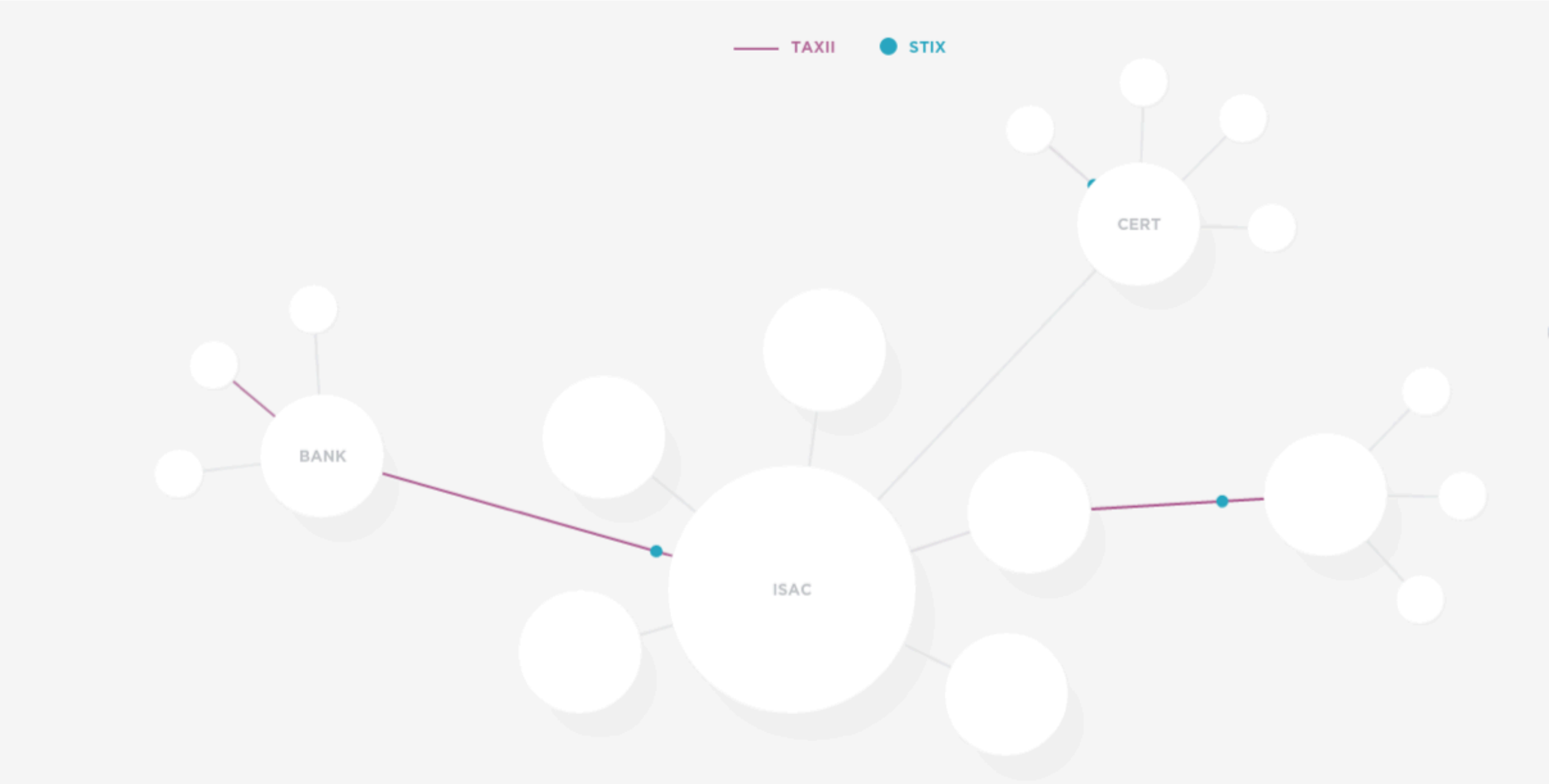
Unfinished intelligence

Tech Intel	Malware Intel
Incidents	Human intell
Open intel	Signals intel

Across geographies

BE AN "ECOSYSTEM": CONNECT PEOPLE

- Step 1: Exchange! Procure!
- Step 2: Understand and empower people, and the diversity of use-cases they have interacting with this information and each-other



ECOSYSTEM BEHAVIOR MEANS CONNECTING

- Machines
- Teams
- Organizations
- People
- Processes
- Competencies
- Investment capability
- Innovation capability
- Etc.

Intelligence is a means by which you can create situational awareness and inform the right stakeholders of the right things, at the right time.

Process

Competencies

Technology

Impact on vendor business models?

False positives?

Where in supply chain does what analysis happen?

?

Q&A