Visibility report
in the ENISA Threat Landscape

Louis Marinos

21 October 2015

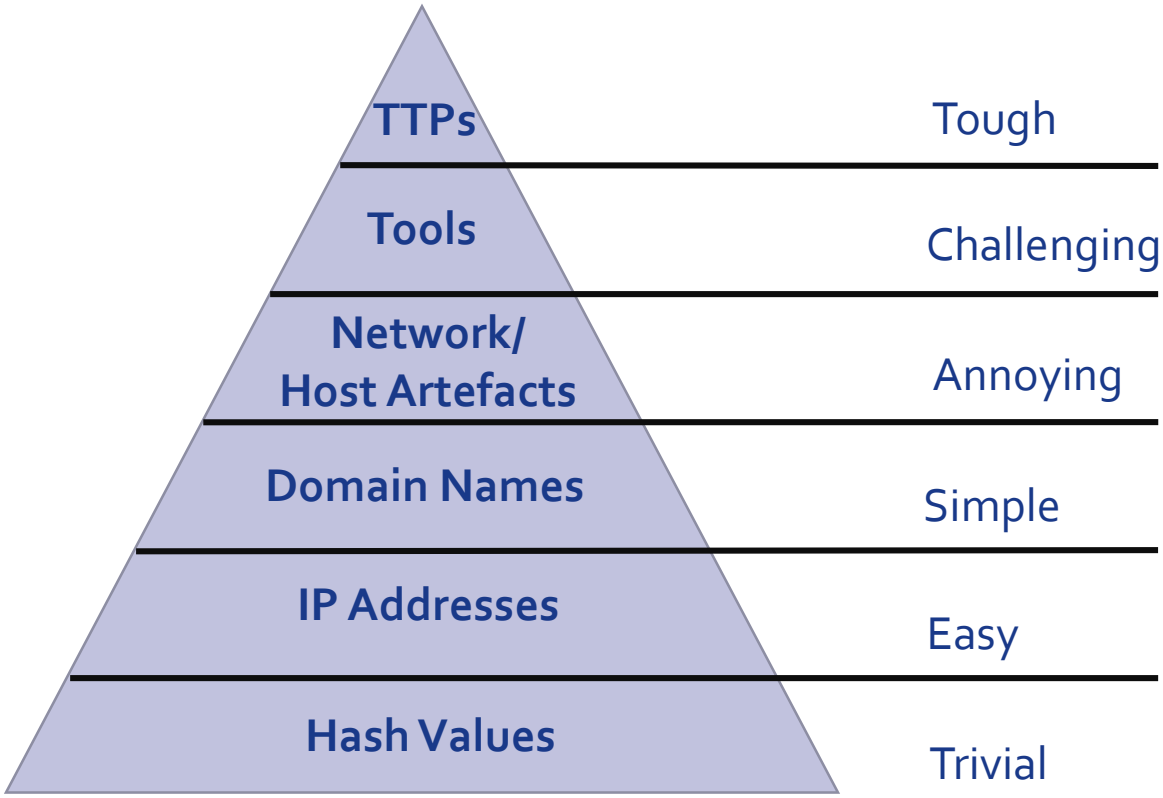
European Union Agency For Network And Information Security

Why ENISA Threat Landscape?

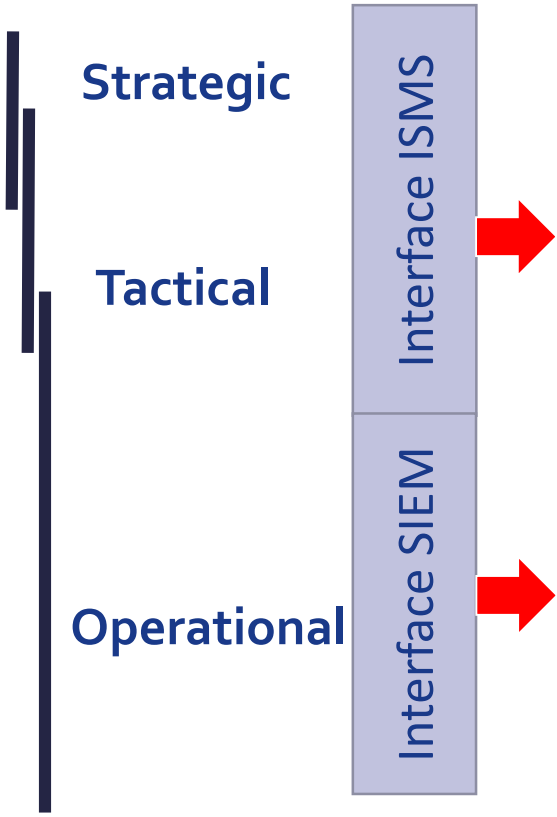
- … raising awareness of potential threats in cyberspace ..(mandate)
- Use available expertise to support Stakeholders in UNDERSTANDING the real threat
- Help developing protection according to the real threats

Information content on cyber threats?

The Pyramid of Pain



Types of information

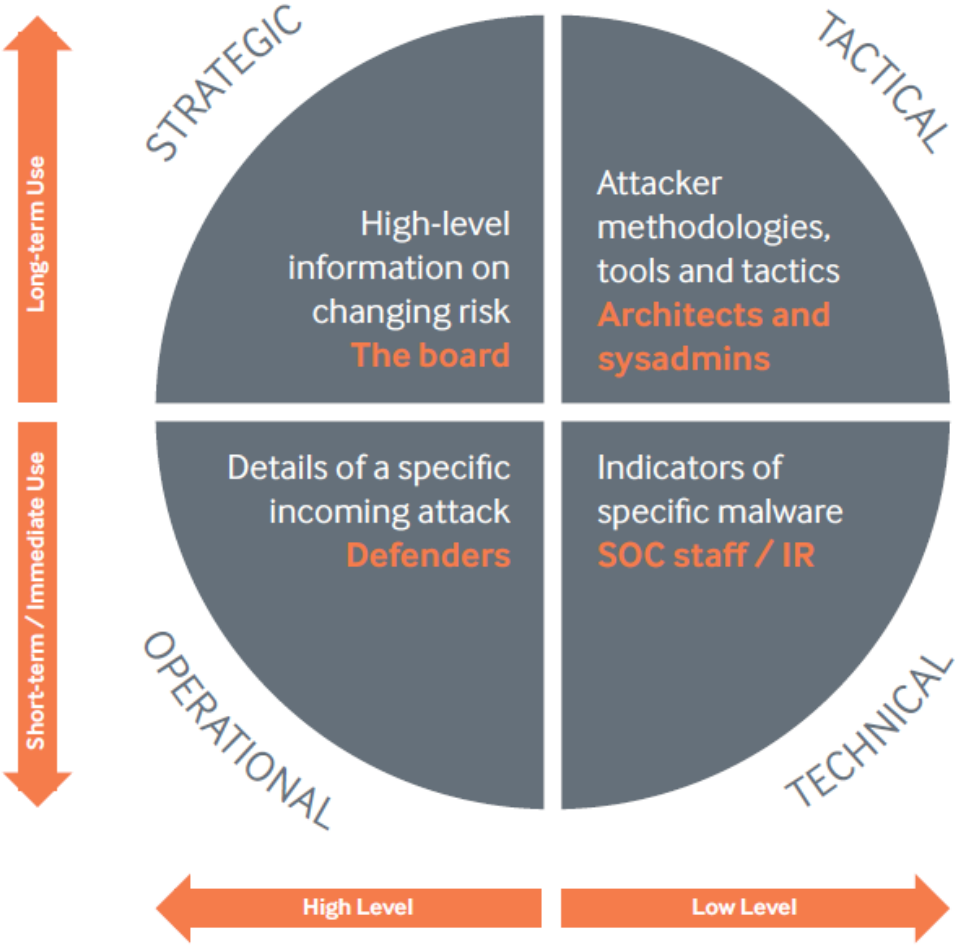


http://detect-respond.blogspot.gr/2013/03/the-pyramid-of-pain.html

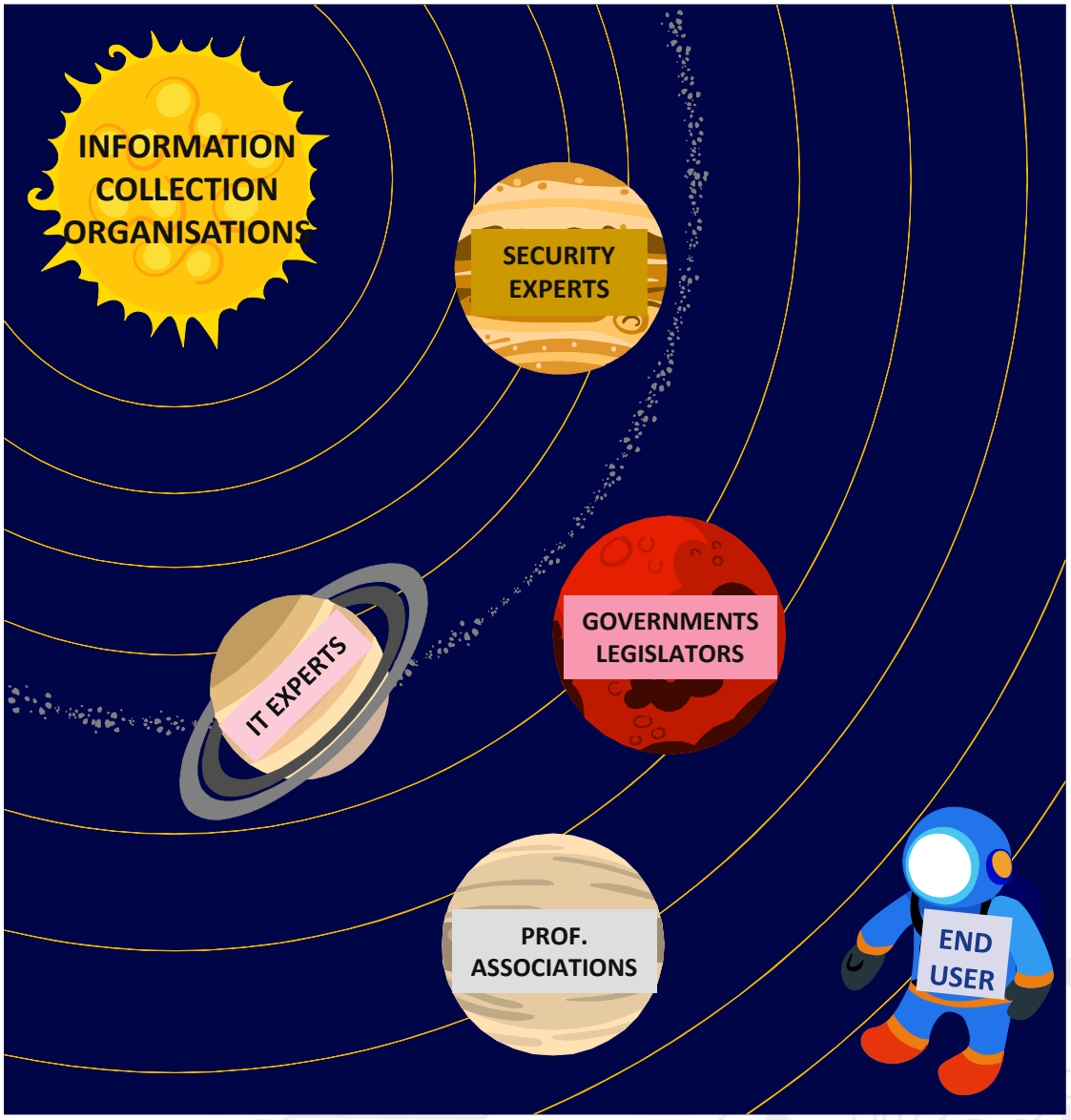
Information content and quality

- **Strategic (S):** the **highest level information about threats**.
  - Created by humans, consumed by humans
  - Lifespan months
- **Tactical (T):** at this level, stakeholders obtain **aggregated information about threats, TTPs** and their elements.
  - Created and consumed by humans and machines
  - Lifespan weeks, months
- **Operational (O):** technical information about incidents, etc.
  - Created by machines, consumed by machines/humans
  - Lifespan days, weeks

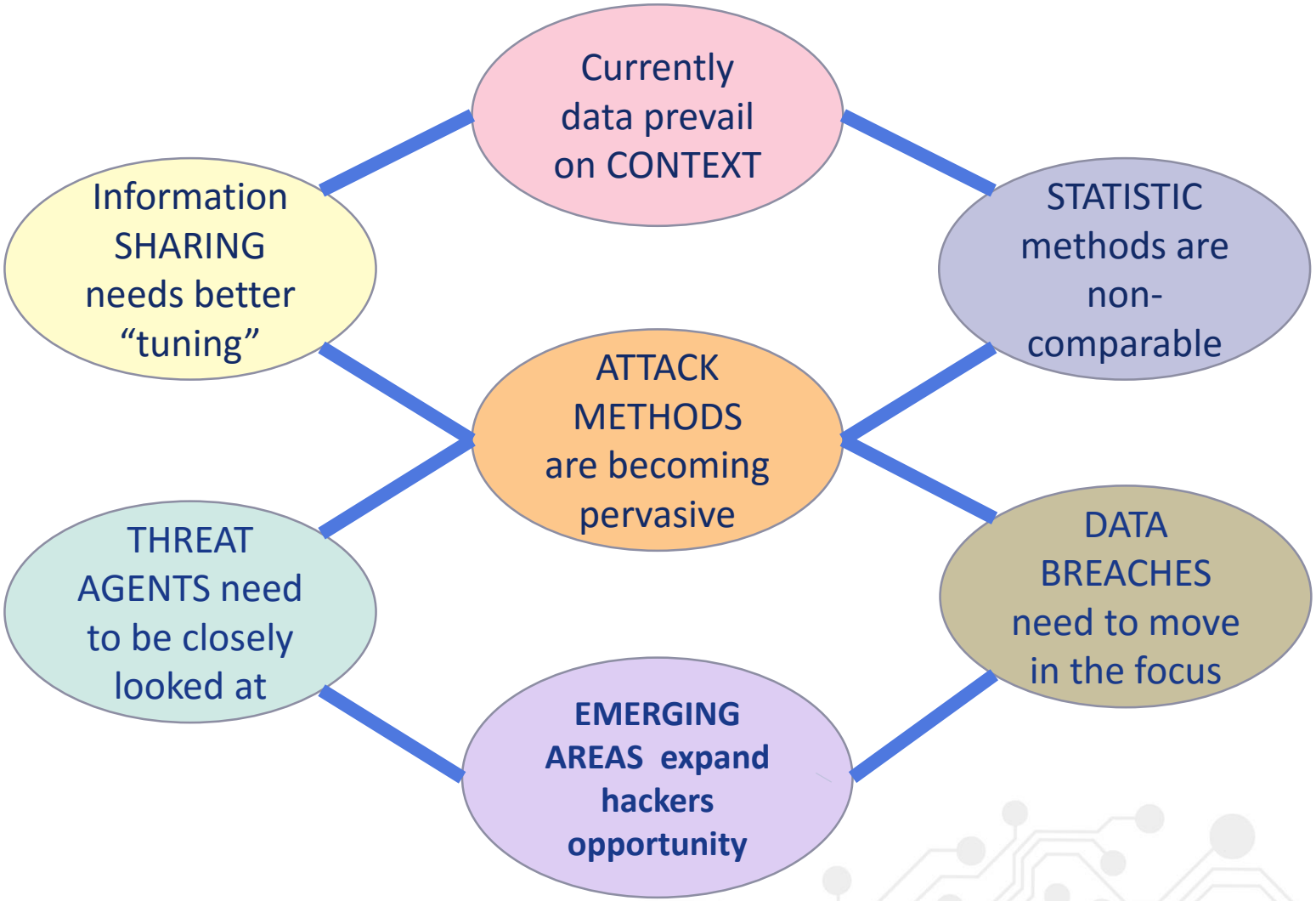
Information content and quality



Levels of cyber threat knowledge



7 “visibility” factors in cyber-space



What exactly?

More long living combined data

CONTEXT

- Moving from data to information is laborious.
- Many data collectors achieve this (MISP).
- Human intervention is required.
- CONTEXT level still low.

Common statistics and metrics models

STATISTICS

- Comparability of statistics is low (e.g x% in 10.000 devices, x% entire malware Trojans, etc.).
- Comparability of metrics also low (importance of incidents, sector, device type, etc.).

Baseline protection guides

ATTACK METHODS

- Attacks tend to cover the high and low ends.
- Most of attack are medium to low tech and yet effective.

Share more contextual, homogenized information

INFORMATION SHARI…

- In some (tested) areas sharing is not fruitful.
- Spread of cyber-attacks is quicker as spread of related intelligence

What more?

Understand who is behind attacks

THREAT AGENTS

- Remove gaps in incident analysis chain.
- Develop data collection methods.
- Re-inforce attribution.

Make Data breach analysis more prominent

DATA BREACH

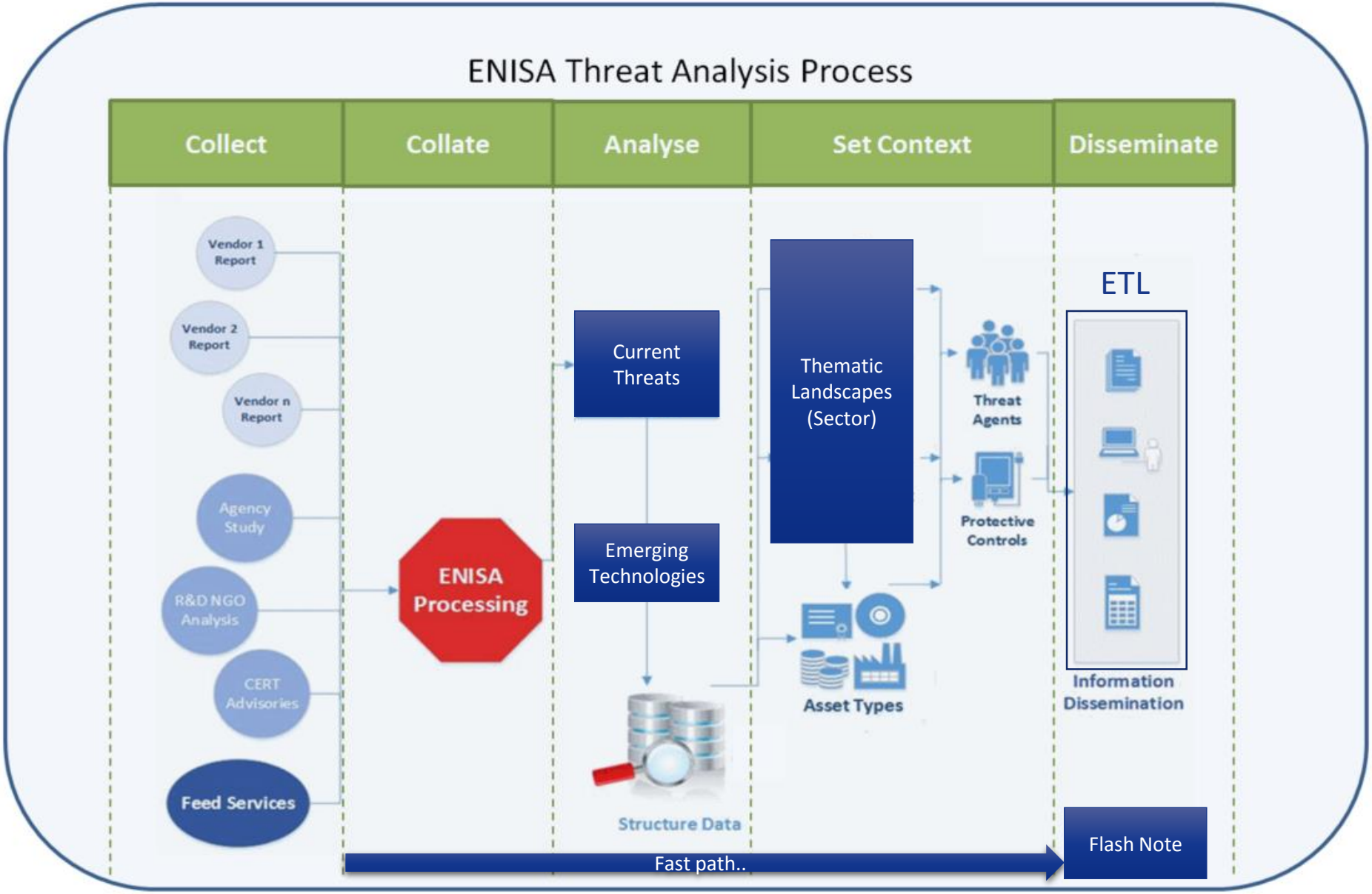
- Security data breach and best lesson learned.
- Data breaches to be reported.
- Data breach analysis as common knowledge source.

Early development of baseline protection

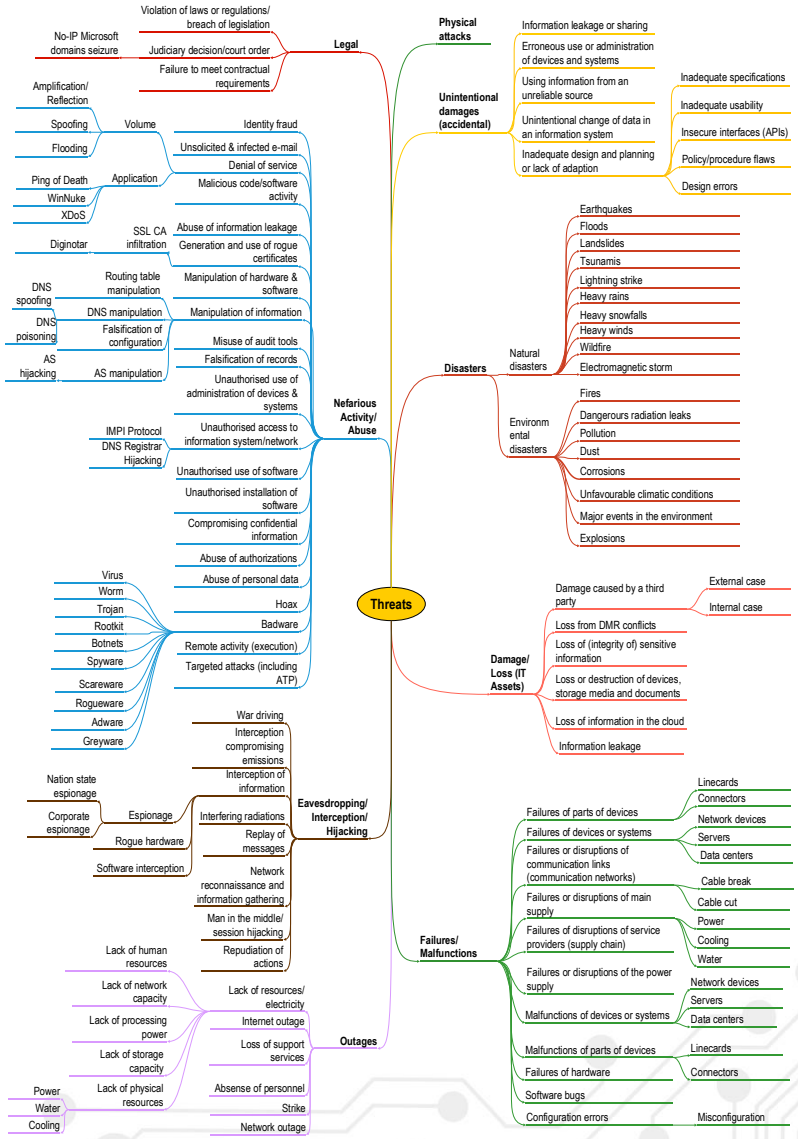
EMERGING AREAS

Quick malicious takeover of exploits.

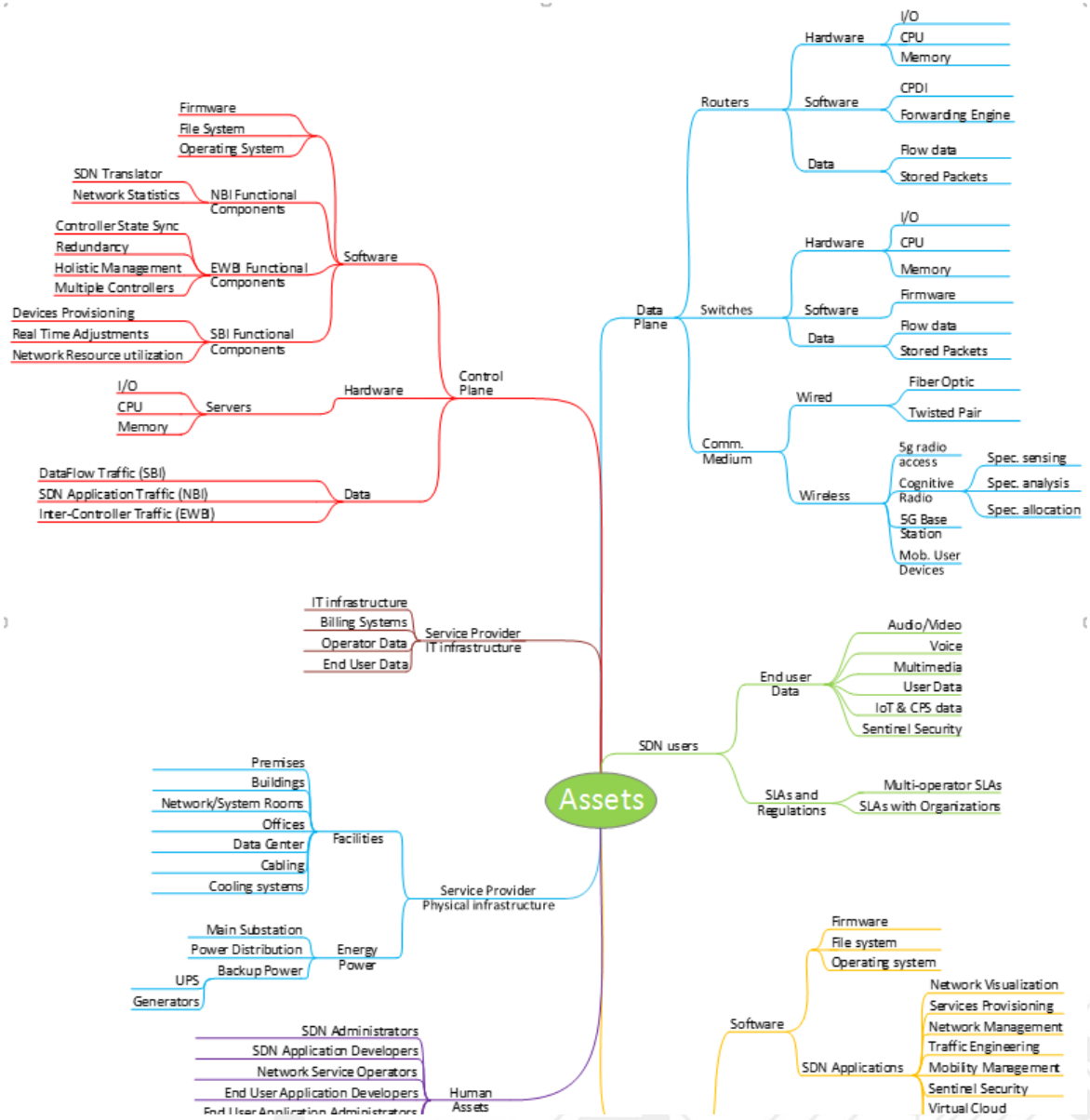
- Security methods immature.
- Technical knowledge (use and misuse cases) initial.


ENISA Threat Analysis Process
Collect
Collate
Analyse
Set Context
Disseminate
Vendor 1 Report
Vendor 2 Report
Vendor n Report
Agency Study
R&D NGO Analysis
CERT Advisories
Feed Services
ENISA Processing
Current Threats
Emerging Technologies
Structure Data
Thematic Landscapes (Sector)
Threat Agents
Protective Controls
Asset Types
ETL
Information Dissemination
Flash Note
Fast path..

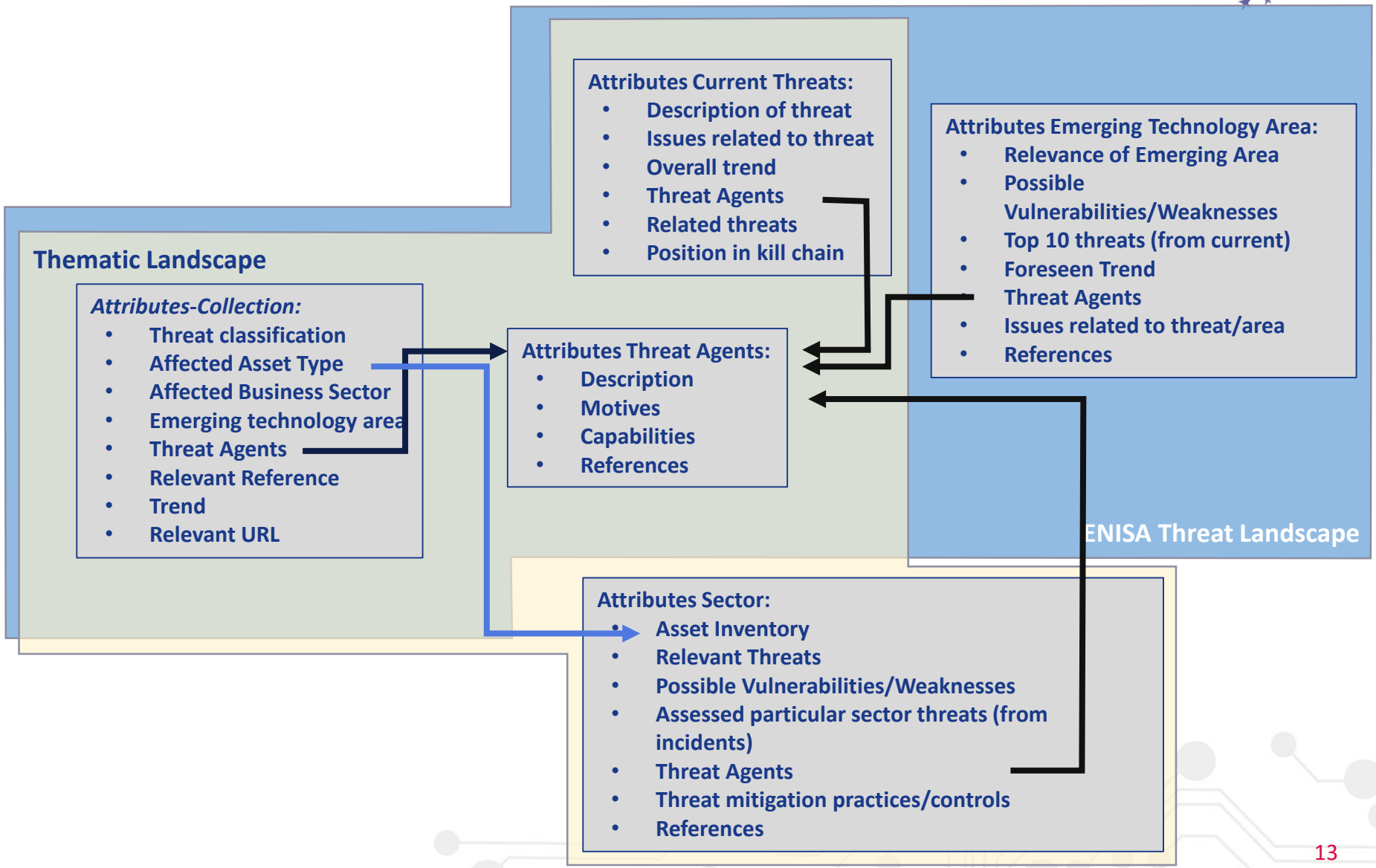
Structure: Better management of input/output..



Structure: Assets (SDN)



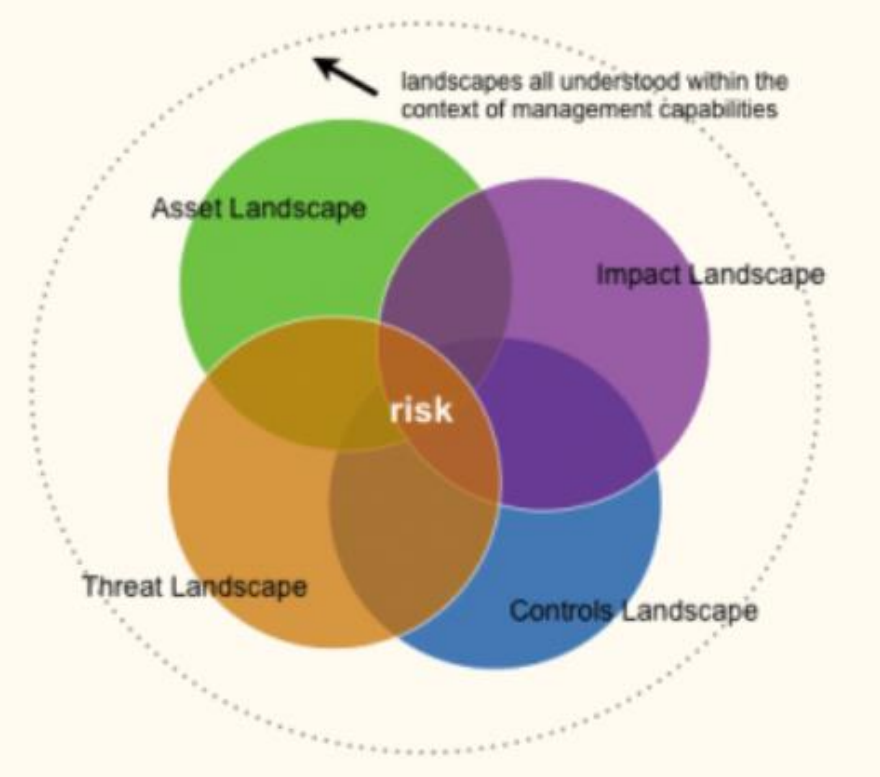
Context is in used model..



Upcoming requirements…

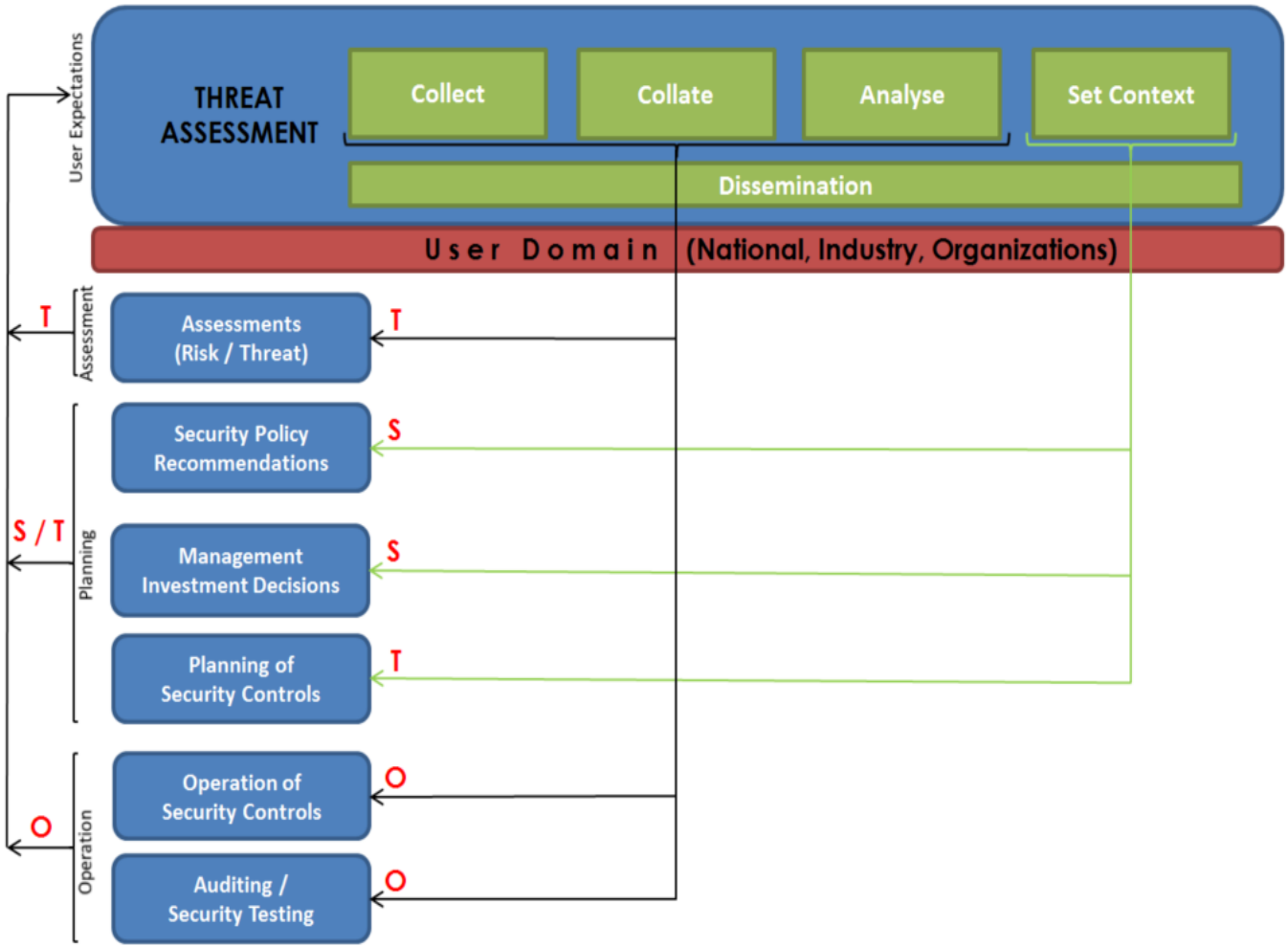
- **Provide hooks to risk assessment, based on this information develop a use case**
- **Develop landscapes for types of organizations (e.g. prosumers/freelancers, SMEs, and government agencies)**
- **Look at main asset types – infrastructure (power+ network+ housing), mobile/fixed endpoints, cloud/web servers, cloud/web applications**
- **Do a risk assessment for each of the above – pointing out the main threats to navigate**
- **Consolidate internal information**
- **Create various views..**

Thematic Landscapes complete the picture



Source: http://veriscommunity.net/veris-overview.html

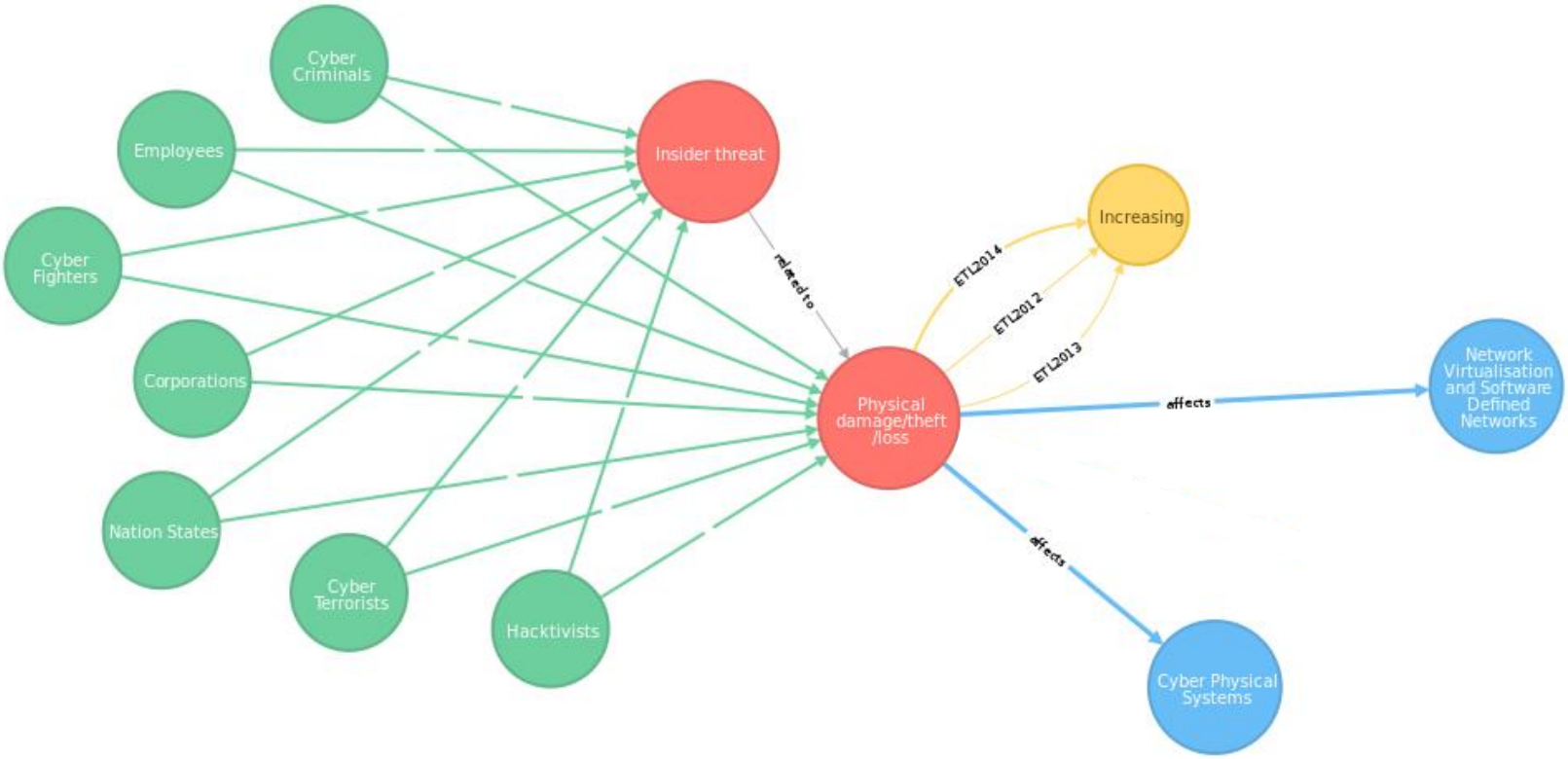
What to do with Threat Information?



Graphics / Presentation

- Presentation/Visualization of results increases use/re-use and efficacy
- It is expected that quite some approaches for presentation of TI will emerge soon.
- Current:
  - Good practices are: Verizon-DBIR, Hackmageddon, Kill-Chain…
  - STIX data format as presentation tool?
  - An interesting/novel approach is project Sinfonier

We experiment on this…



Takeaways…

- For users:
  - Understand the scope of your assessments
  - Identify threat exposure and understand what you can afford
  - Build TI tool usage models according to points above
  - Increase agility of assessments and ISMS
  - Think that current state of TI is still initial BUT has a great potential
- For providers:
  - Establish usable information according to requirements
  - Increase structuring / follow user needs
  - Facilitate visualization, data re-use, historical data
  - Interconnect with ISMS / increase agility
- For ENISA:
  - Cooperation
  - Create data
  - Check the hook to ISMS

..thank you for your attention..

L. Marinos
louis.marinos@enisa.europa.eu