

ENISA Threat Landscape: Risk Management facilitation

Louis Marinos| Threat/Risk Analyst

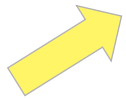
Swiss Cyber Risk Research Conference 2016

European Union Agency for Network and Information Security

Threat Intelligence is key to all sectors of ISMS/Risk Management:

Dynamicity

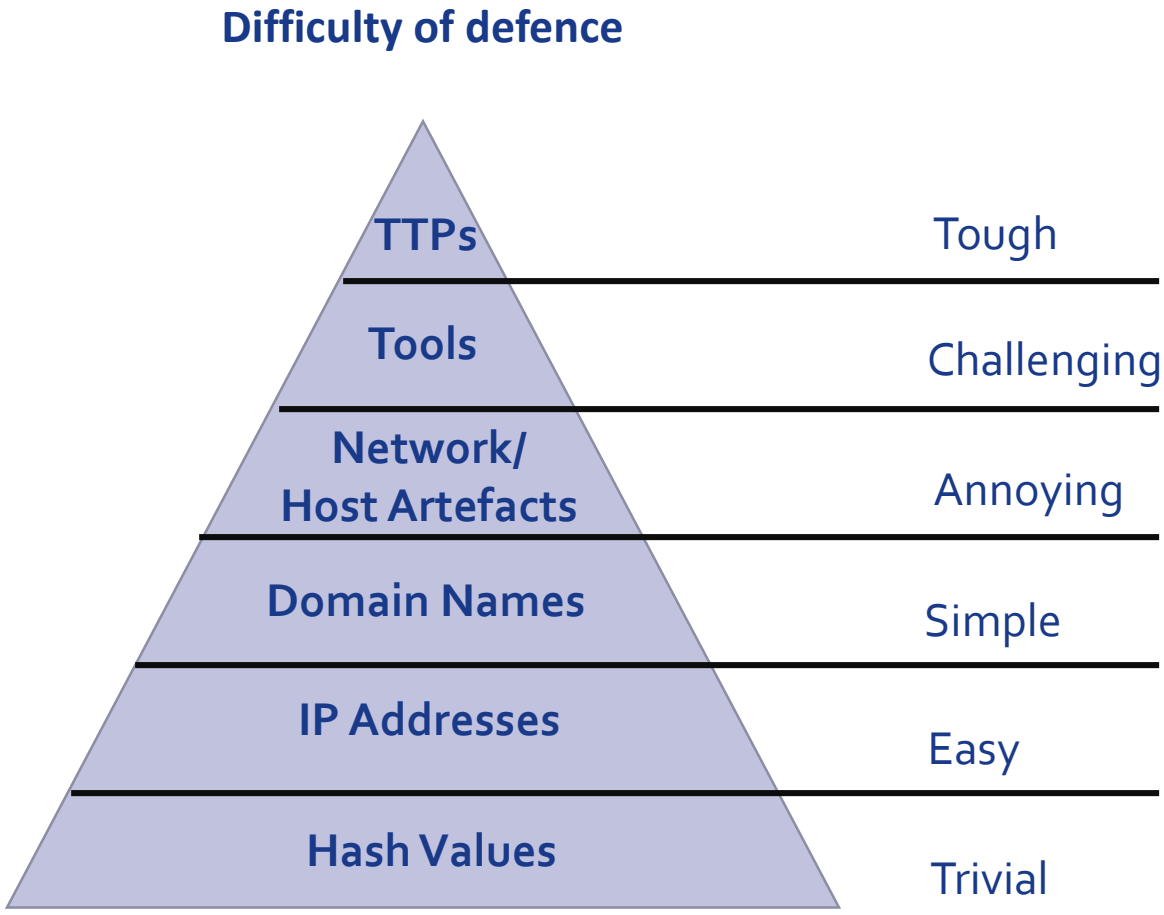
Risk: [Asset, Vulnerabilities, Controls],

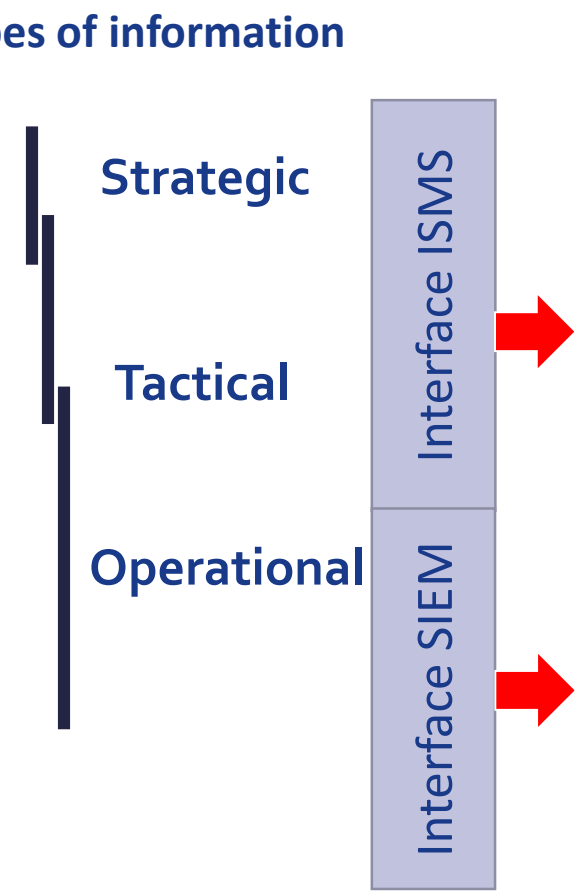


[Threat, Threat Agent],

[Impact, Value, Influence]

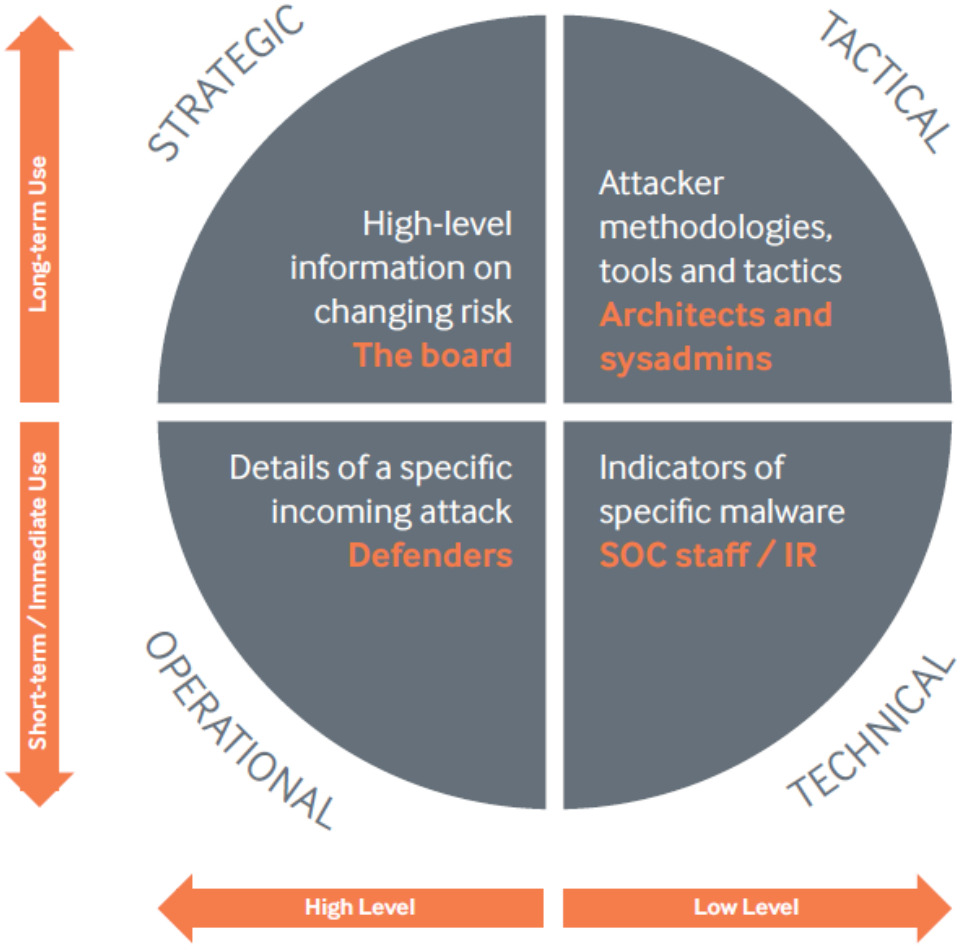
Threat Information is a pyramid



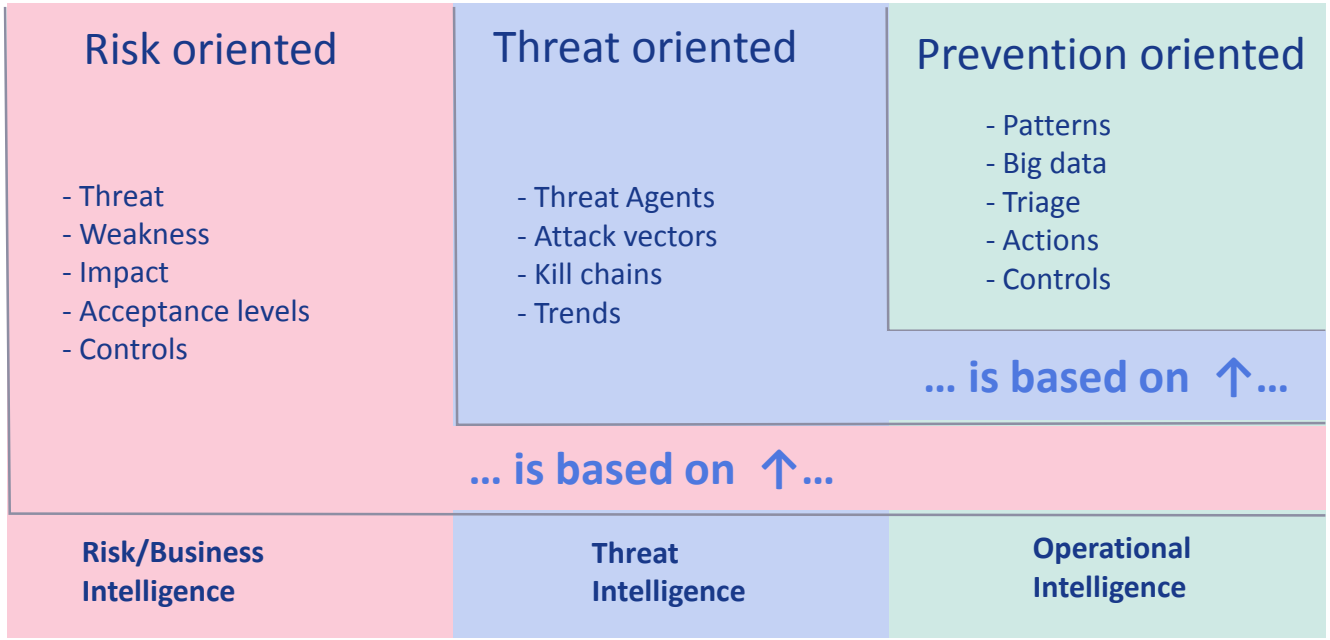


http://detect-respond.blogspot.gr/2013/03/the-pyramid-of-pain.html

Threat Landscape/Intell Overview



Positioning Threat Intelligence



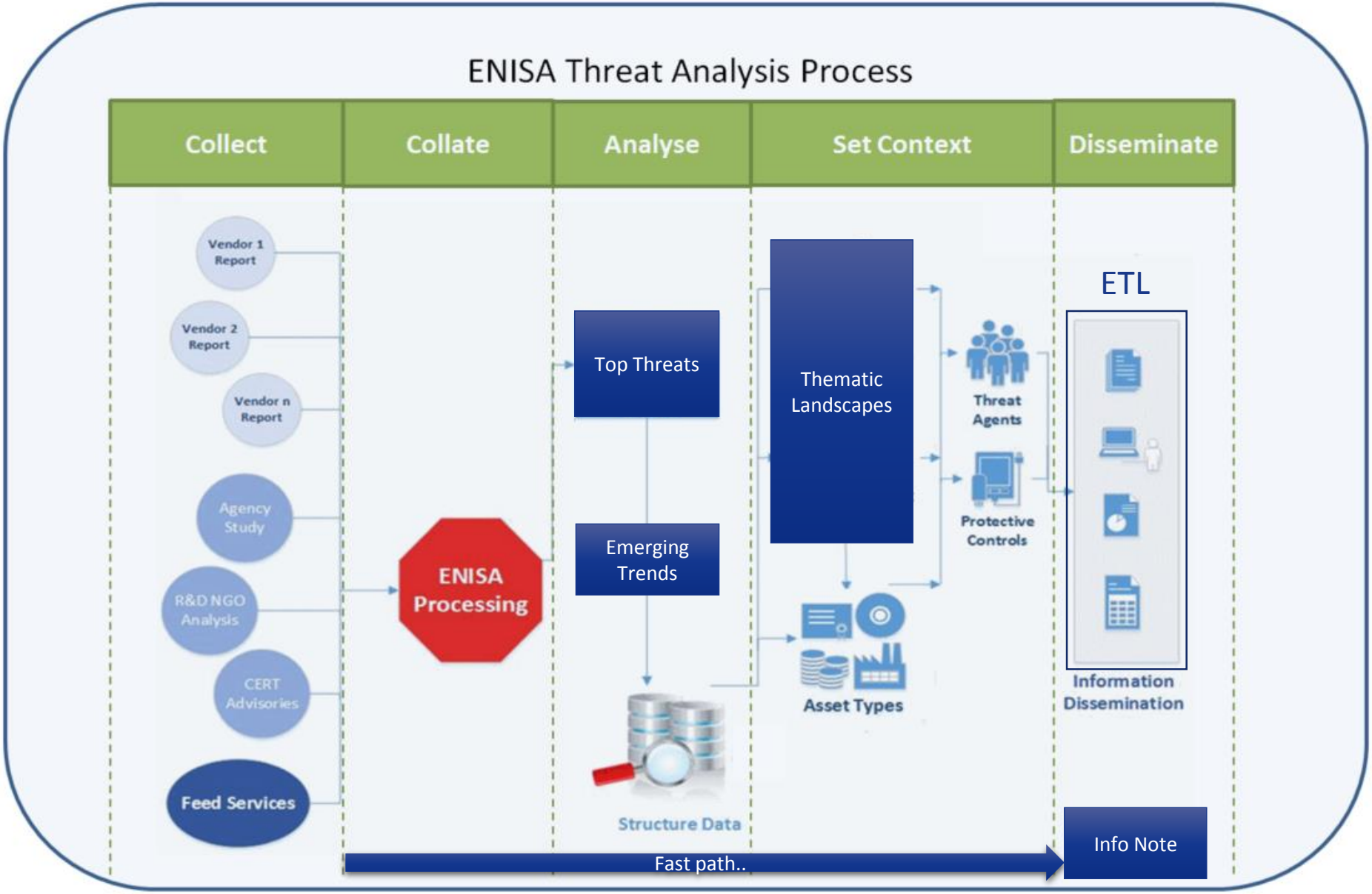
We need to ***increase*** reaction speed at all levels!

The ENISA Threat Landscape

The ENISA Threat Landscape provides an overview of threats and current and emerging trends.

It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends.

Over 380 recent reports from a variety of resources have been analyzed.


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
Top Threats
Emerging Trends
Structure Data
Thematic Landscapes
Threat Agents
Protective Controls
Asset Types
ETL
Information Dissemination
Info Note
Fast path..

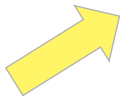
Topics covered:

Risk: [Asset, Vulnerabilities, Controls],

[Threat, Threat Agent],

[Impact, Value, Influence]

Dynamicity



The top threats

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	→	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	→	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓

HIGHLIGHTS: GOOD STUFF

- Orchestrated actions to take down malicious infrastructure and analyse incidents to increase attribution.
- Strengthening of governmental awareness, cyber-defence expenses, capabilities and level of cooperation among states.
- Many developments in threat intelligence: proliferation of information sharing, tools and products to enhance awareness, preparedness and efficiency of defence.
- R&D to accommodate changes of the cyber-threat landscape to existing protection measures and methods and tools.

HIGHLIGHTS: NOT SO GOOD

- Persistent attacks based on hardware, far below the “radar” of available defence tools and methods.
- Enhancements in the provision of “cyber-crime-as-a-service”, tool developments for non-experts and affiliate programmes.
- Highly efficient malware weaponisation and infection tools based on detected vulnerabilities.
- Highly profitable operation of malicious infrastructures and malware campaigns to breach data and ransom.

POLICY CONCLUSIONS

- Make threat intelligence inherent part of the national cyber-defence capabilities.
- Perform analysis of reported incidents and recycle results for better planning of defences.
- Disseminate cyber-threat knowledge to all players in cyber-space.

BUSINESS CONCLUSIONS

- Simplify content of threat intelligence to achieve wider dissemination in the stakeholder community.
- Elaborate on threat agent models and make it inherent part of threat intelligence.
- Create correlated, contextualized threat information to increase timespan and relevance.
- Invest in better vulnerability management and exploitation of dark web.

RESEARCH CONCLUSIONS

- Develop applied statistic models to increase comparability of cyber-threat and incident information.
- Develop new models for seamlessly operated security controls to be included in complex, smart end-user environments.
- Develop trust models for the ad hoc interoperability of devices within smart environments.

Security Community: GO INNOVATE!

- Right-place Threat Intel
  (enable it within companies of any size)
- Apply landscaping principles
  (risks, assets, protection)
- Use threat landscaping to test protection (simulate reality)

Thank you for your attention

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu