



# Threat Landscape 2015

*“Το τοπίο των κυβερνοκινδύνων για το 2015”*

Louis Marinos | NIS Expert

1 April 2015



# Subject of the talk

The motto of 5<sup>th</sup> Infocom Security:

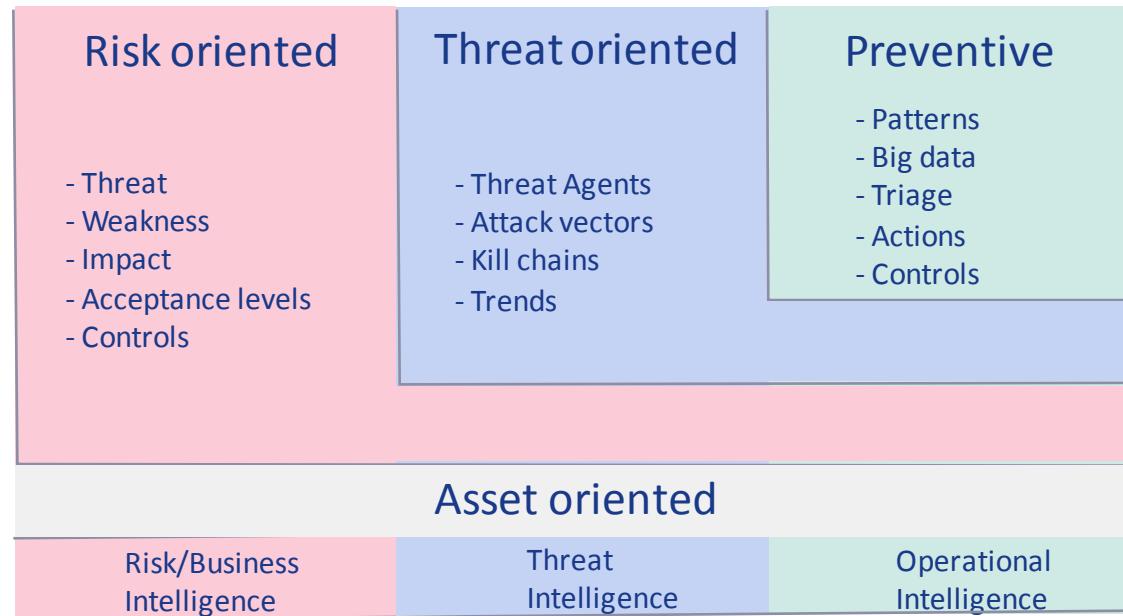
## Mind the Risk. Be proactive!

Define protection needs

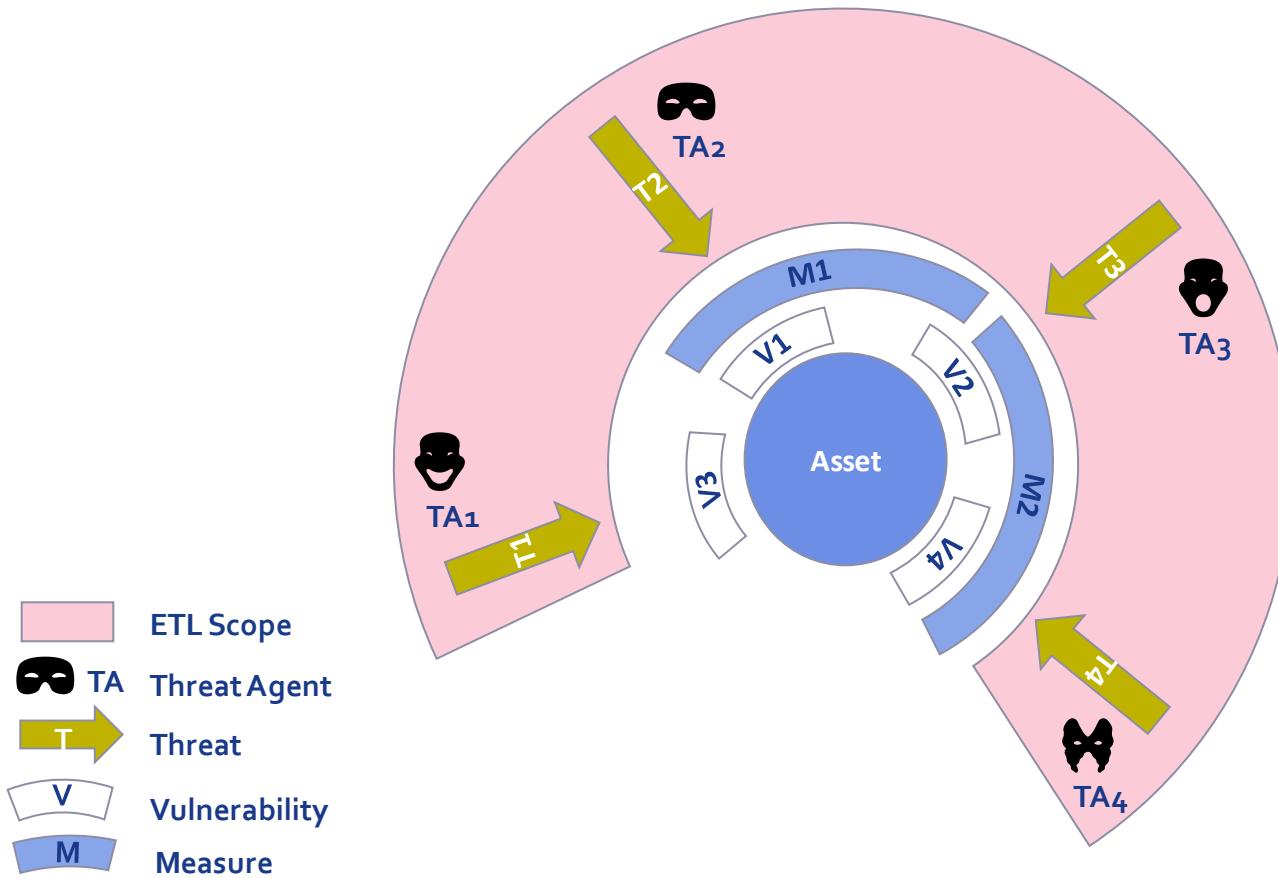
Adapt your defences



# Risks, assets, threats, defences...



# Cyber-Threats/Risks: Basic assumption



Birth of Risks to assets: their exposure to threats

# ETL Scope: What are the parts?



Threats

Threat Agents

Attack methods (vectors)

Assets

(Mostly technical) Vulnerabilities

Controls

...and interconnections thereof

Our internal **Cyber Threat Intelligence!**

**CAUTION: TI IS NOT REPLACEMENT OF RISK MANAGEMENT**



# Threat Information vs. Intel.



## Information versus Intelligence

Information	Intelligence
- Raw, unfiltered feed	- Processed, sorted information
- Unevaluated when delivered	- Evaluated and interpreted by trained Intelligence Analysts
- Aggregated from virtually every source	- Aggregated from reliable sources and cross correlated for accuracy
- May be true, false, misleading, incomplete, relevant or irrelevant	- Accurate, timely, complete (as possible), assessed for relevancy
- Not actionable	- Actionable



# Information types of Threat Intel.



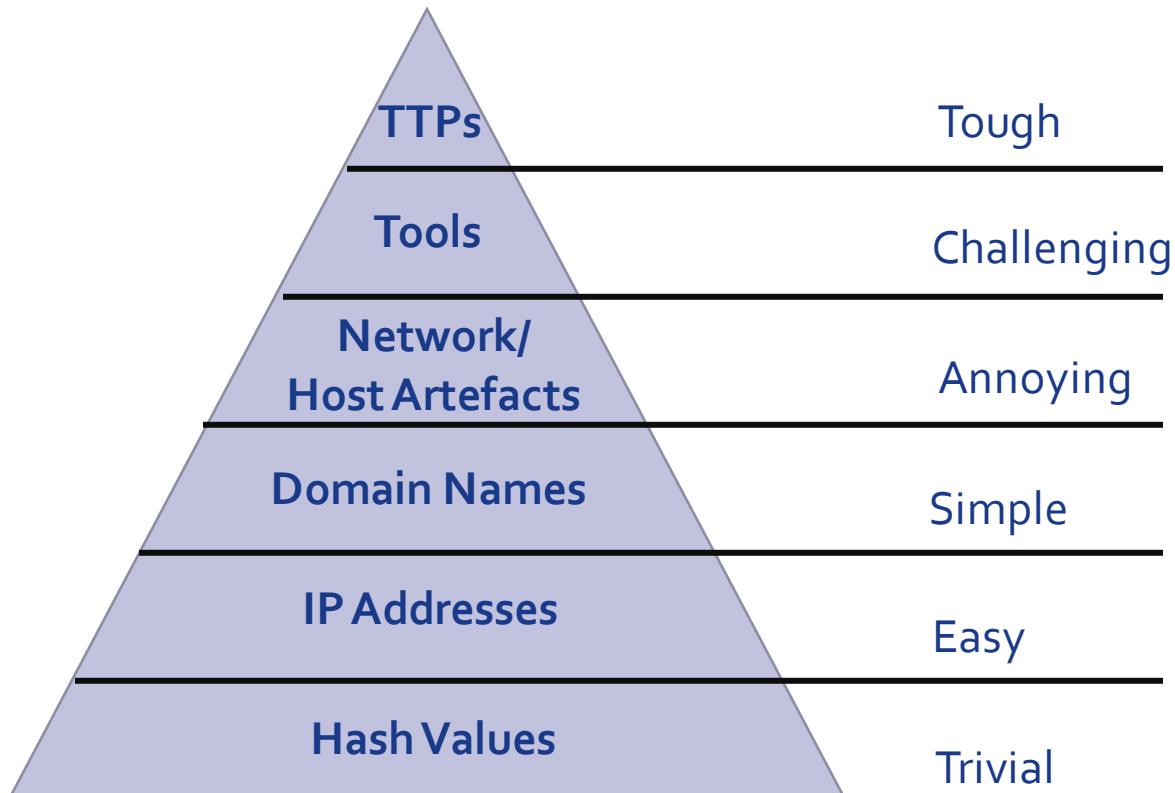
- **Strategic (S):** the **highest level information about threats.**
  - Created by humans, consumed by humans
  - Lifespan months
- **Tactical (T):** at this level, stakeholders obtain **aggregated information about threats** and their elements.
  - Created and consumed by humans and machines
  - Lifespan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



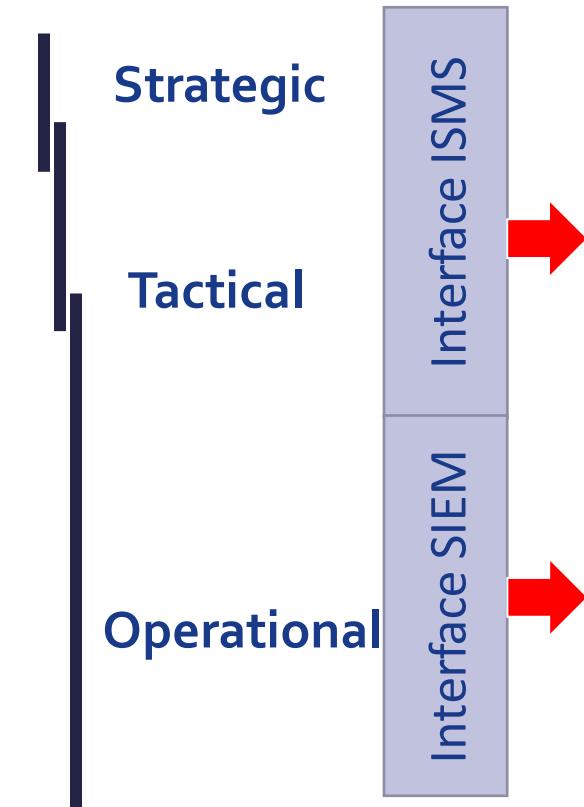
# Why do we need to know?



The Pyramid of Pain

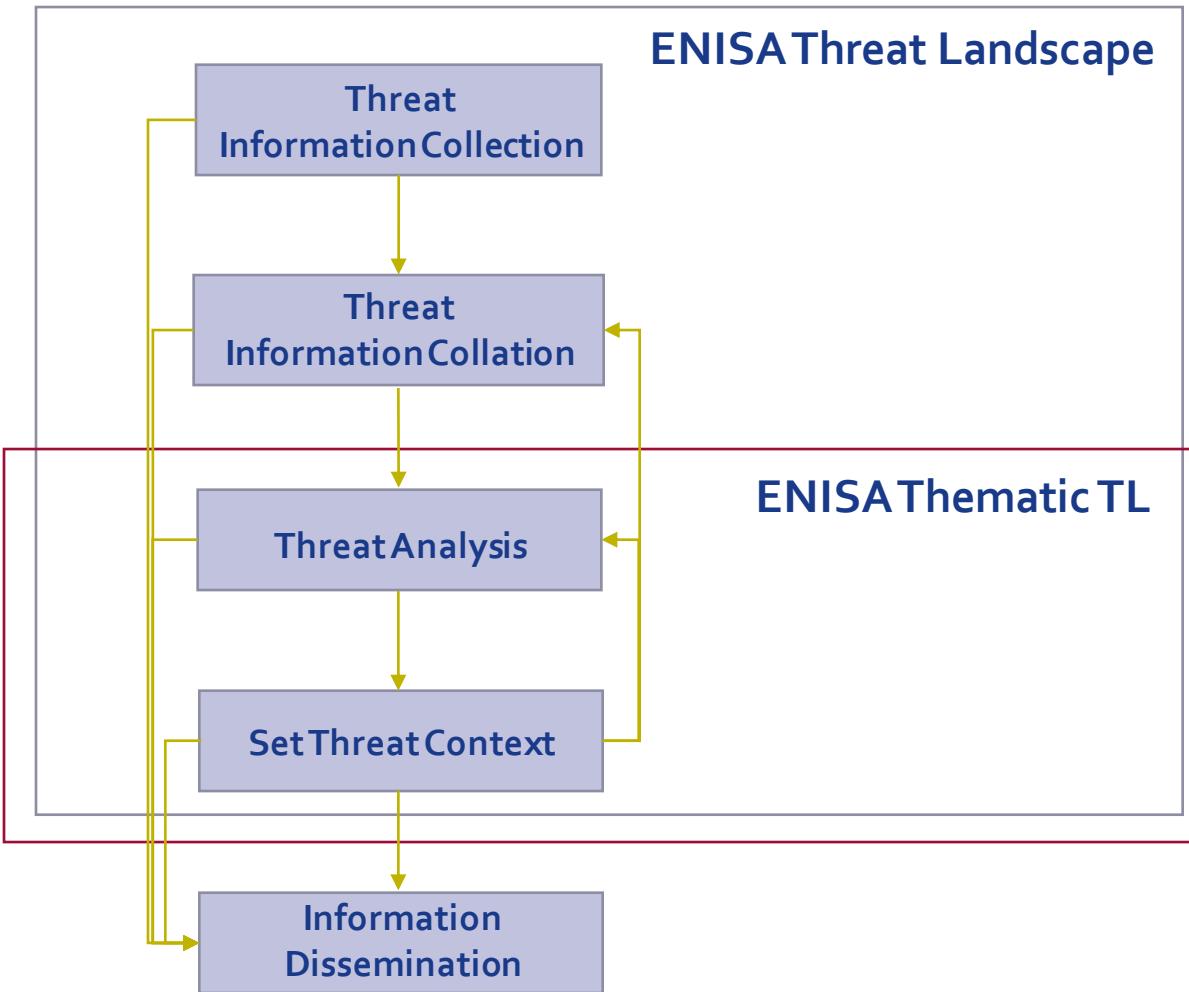


Types of information



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

# From Threat Info to Intel...



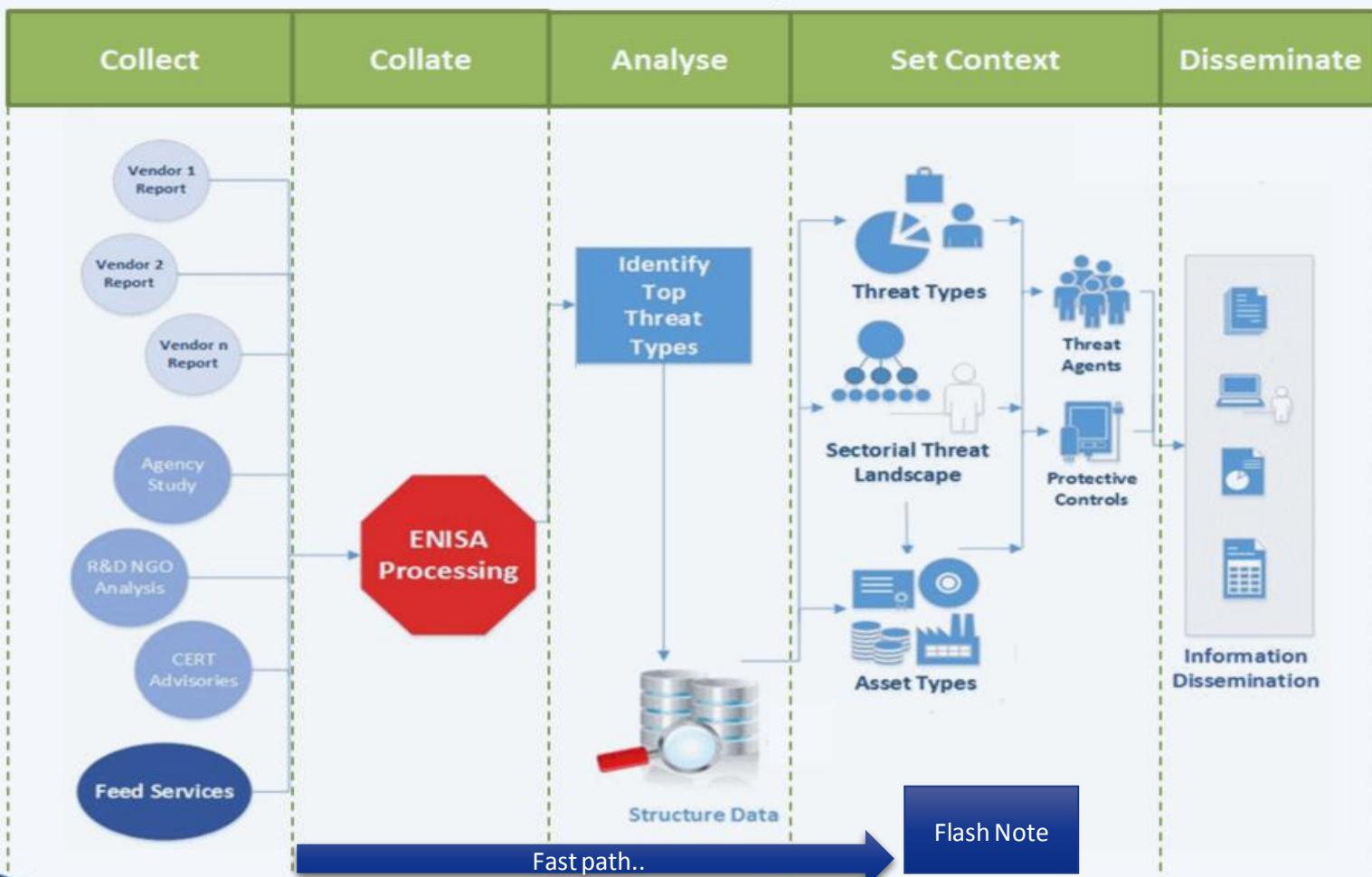
Find reliable sources

Isolate and relate similar information

Evaluate findings and decide what to take on board

Find out practices, issues, vulnerabilities, risks, etc.

# How does ENISA do it?



# Top Threats and Trends

Top Threats 2013	Assessed Trends 2013	Top Threats 2014	Assessed Trends 2014	Change in ranking
1. Drive-by downloads (renamed to Web-based attacks)	↑	1. Malicious code: Worms/Trojans	↑	↑
2. Worms/Trojans	↑	2. Web-based attacks	↑	↓
3. Code Injection	↑	3. Web application /Injection attacks	↑	→
4. Exploit Kits	↑	4. Botnets	↓	↑
5. Botnets	↔	5. Denial of service	↑	↑
6. Physical Damage/Theft/Loss	↑	6. Spam	↓	↑
7. Identity Theft/Fraud	↑	7. Phishing	↑	↑
8. Denial of Service	↑	8. Exploit kits	↓	↓
9. Phishing	↑	9. Data breaches	↑	↑
10. Spam	↔	10. Physical damage/theft /loss	↑	↓
11. Rogueware/Ransomware / Scareware	↑	11. Insider threat	↔	(NA. new threat)
12. Data Breaches	↑	12. Information leakage	↑	↑

# Impressive facts: clear text

**Web is the most popular platform for malware distribution:** "*Malicious URL is by far the first malicious object detected (72,9%)*" Ref: (Kaspersky IT Threat Evolution Q2 2014, findings overview:

<http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/>)

**Mail is another important channel for malware distribution:** "*Of the e-mail traffic, 13.7% contained malicious URL*"

Ref: Symantec Intelligence Report May 2014, <http://www.symantec.com/connect/blogs/symantec-intelligence-report-may-2014>

**Attacks become more effective and targeted:** "*Mobile banking Trojans have increased by almost factor four over the year. Since July 2012 14,5 Times*" Ref: (Kaspersky IT Threat Evolution Q2 2014, findings overview:

<http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/>)

**2014 the year of data breach?** "*57% of the significant data loss over the past decade resulted from what could be termed sloppiness*" Ref: [http://capgemini.ft.com/web-review/sloppiness-to-blame-for-more-data-losses-than-hacking-study-claims\\_a-41-648.html](http://capgemini.ft.com/web-review/sloppiness-to-blame-for-more-data-losses-than-hacking-study-claims_a-41-648.html), relevant report

<http://cmds.ceu.hu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope.pdf>

**Efficiency of existing controls needs to be increased:** "*54% of malware goes undetected by Antivirus products*"

Ref: NTT Global Threat Intelligence Report 2014 (<http://www.nttcomsecurity.com/en/services/managed-security-services/threatintelligence/>)

**Sophistication of malware and attacks increases:** "*In 2013, 30% of malware samples used custom encryption to steal data.*"

Ref: WebSense Threat Report 2014, <http://www.websense.com/content/websense-2014-threat-report.aspx>

# Take aways...

- 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



# Concluding...

- Knowledge can be obtained by aggregating and correlating information (needs brain power)
- Skill is an amount of knowledge on a certain subject matter (capability building)
- A lot of skill is needed in the area of cyber threat intelligence (skill management)
- Try to find the right mix (make or buy decisions)
- Look for upcoming automation/tool developments
- The area has great potential



**Thank you for your attention....**

[louis.marinos@enisa.europa.eu](mailto:louis.marinos@enisa.europa.eu)

