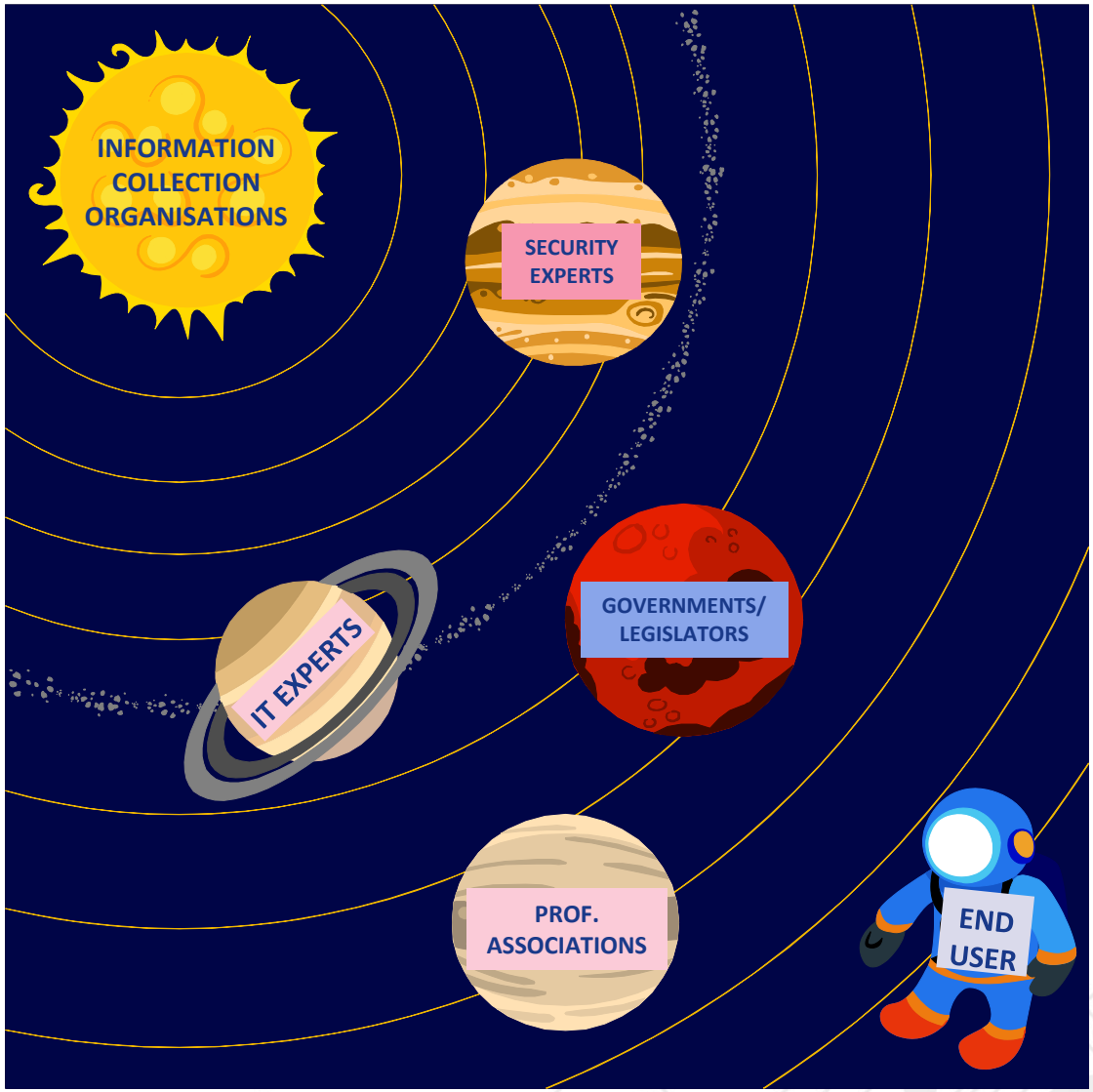


ENISA Threat Landscape 2015: More with Less

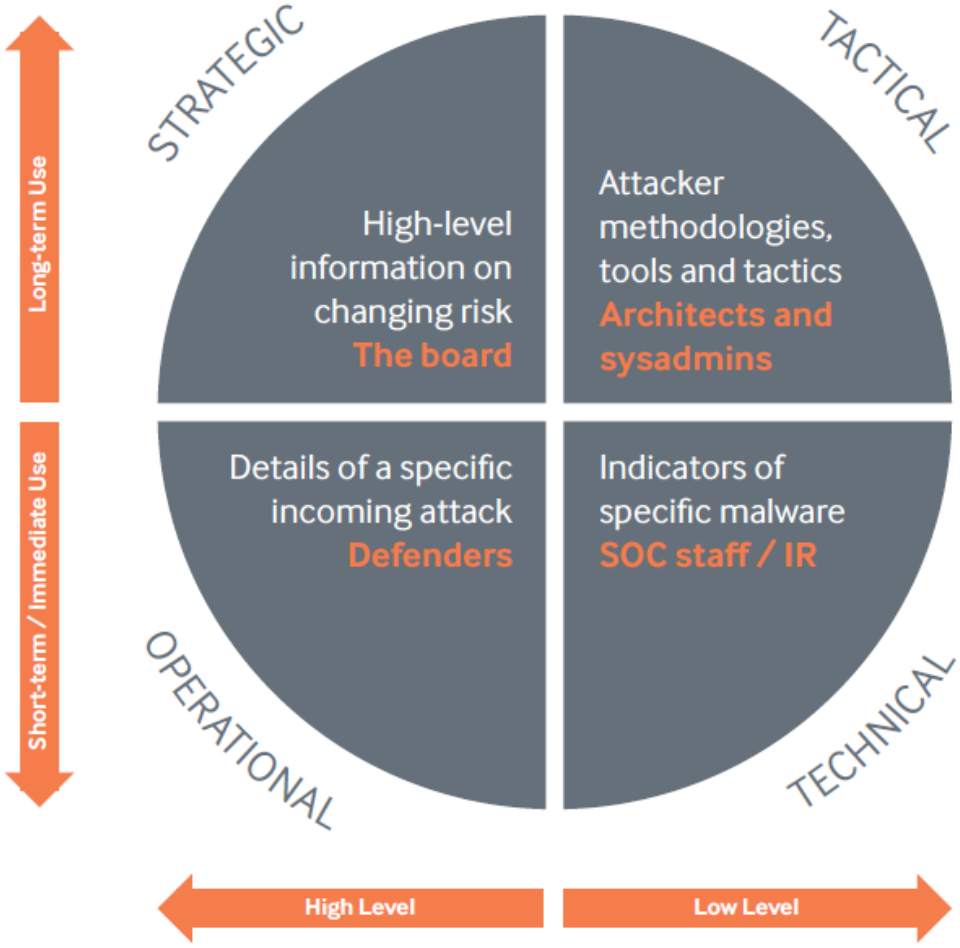
Louis Marinos| ENISA Risk/Threat Analysis

European Union Agency for Network and Information Security

SECURITY KNOWLEDGE: THE GRAVITY IN CYBER SPACE



Threat Landscape/Intell Overview



Threat Intel Definition

[it is] evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets ..

(CERT-UK): *https://www.cert.gov.uk/wp-content/uploads/2015/03/An-introduction-to-threat-intelligence.pdf*

A threat landscape is much less…

- Much less data (though based on massive data)
- Much less tech (reducing to the understandable)
- Much less details (reducing to the relevant)

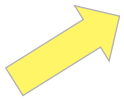
And therefore is much more…

- It is comprehensive (consists of context)
- Lasts longer (more generic/systemic conclusions)
- Targets the board (has business relevance)

Threat Intel is key to security:

Dynamicity

Risk: [Asset, Vulnerabilities, Controls],



[Threat, Threat Agent],

[Impact, Value, Influence]

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)

Security Community: GO INNOVATE!

- Work on presentation models
  (hide complexity, increase intuition)
- Deliver robust statistics models
  (none of the incident data statistics are same)
- Investigate Threat Agent models/data
  (we know only a few about them)

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	↑	↓

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