Το τοπίο των κυβερνοαπειλών: παρούσα κατάσταση και τάσεις

Louis Marinos

European Union Agency for Network and Information Security

GOOD NEWS..

CTI getting mainstream..

EUROPEAN
COMMISSION

Strasbourg, 26.3.2019
C(2019) 2335 final

COMMISSION RECOMMENDATION

of 26.3.2019

Cybersecurity of 5G networks

A coordinated European risk assessment

(8) Member States should exchange information with each other and with relevant Union bodies for the purpose of building a common awareness of the existing and potential cybersecurity risks associated with 5G networks.

(9) Member States should transmit their national risk assessments to the Commission and to the European Agency for Cybersecurity (ENISA) by 15 July 2019.

(10) The European Agency for Cybersecurity (ENISA) should complete a specific 5G networks threat landscape mapping. The Cooperation Group and the Computer Security Incident Response Teams network set up under Directive (EU) 2016/1148 should support this process.

(11) Taking into account all these elements and by 1 October 2019, Member States with

..AND BAD NEWS..

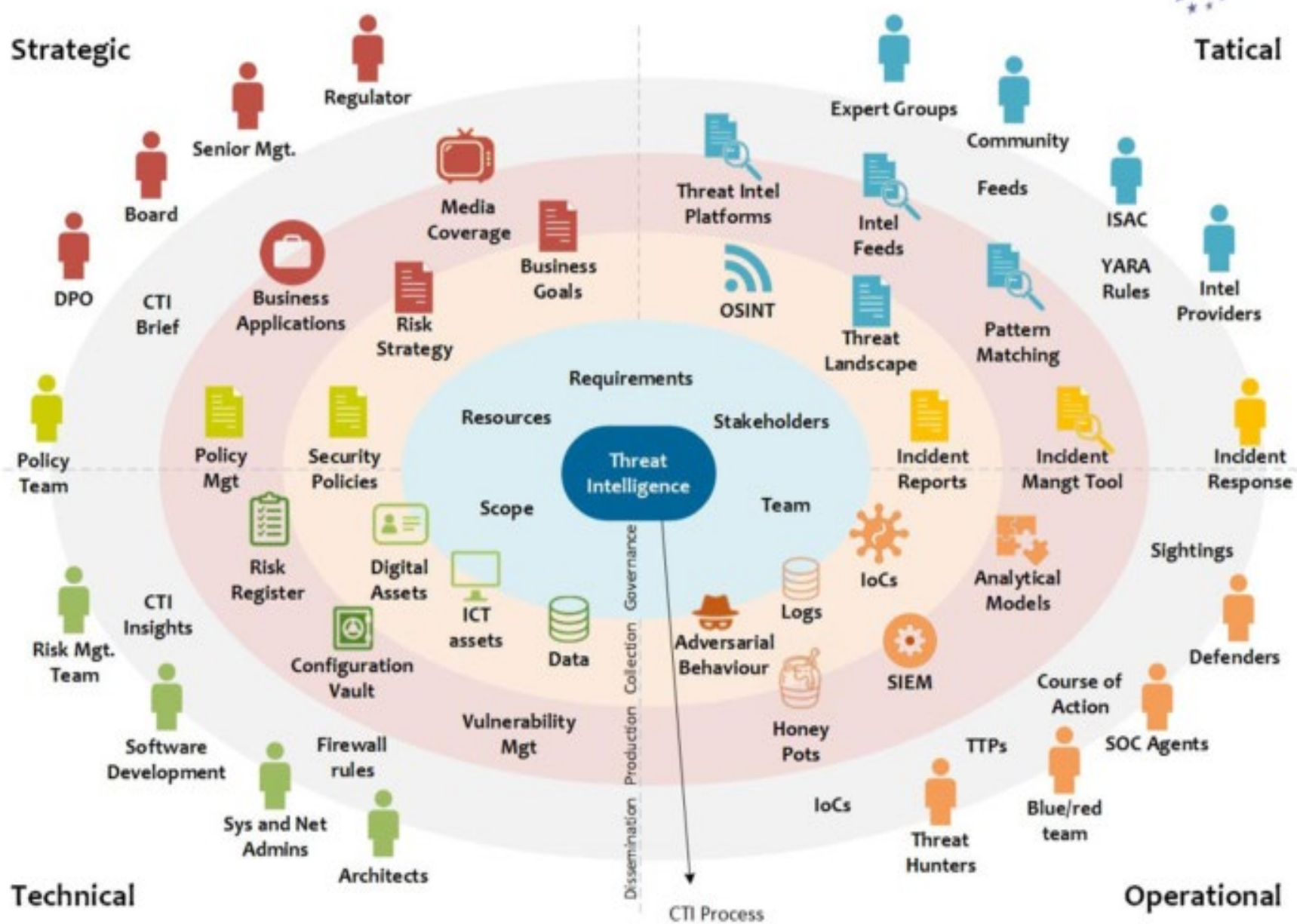
Threat Landscapes (and CTI) are costly…

WHAT IS CYBERTHREAT INTELLIGENCE?

Ready to use information on cyber-threats

- Real-time feeds on cyberthreats including:
  - Indicators of compromise
  - (Technological) Assets targeted
  - Vulnerabilities/weaknesses exploited
- Information regarding attack vector
- Actionable information on mitigation
- Trends of individual threat types (various levels: technical, tactical, strategic)
- Information on threat agents

Cyber Threat Intelligence Program



CTI AND STAKEHOLDERS

Reference: Andreas Sfakianakis
https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/lets-make-cti-great-again-cti-eu-final.pdf/view

CURRENT STATUS OF MATURITY OF CTI

	CYBER THREAT INTELLIGENCE	INCIDENT RESPONSE	SECURITY OPERATIONS
Adoption	Early adoption phase	Mainstream since ~2010	Mainstream since ~2005
Focus	External threat monitoring	Security incidents and risk escalation	Notable security event monitoring
Best practices	Evolving best practices	Mature best practices	Mature best practices
Technology enablement	Limited technology enablement	Mature technology enablement	Mature technology enablement

Reference:
eclectic iq

CTI IS AGILITY

agility and rigid processes

ENISA THREAT LANDSCAPE 2018

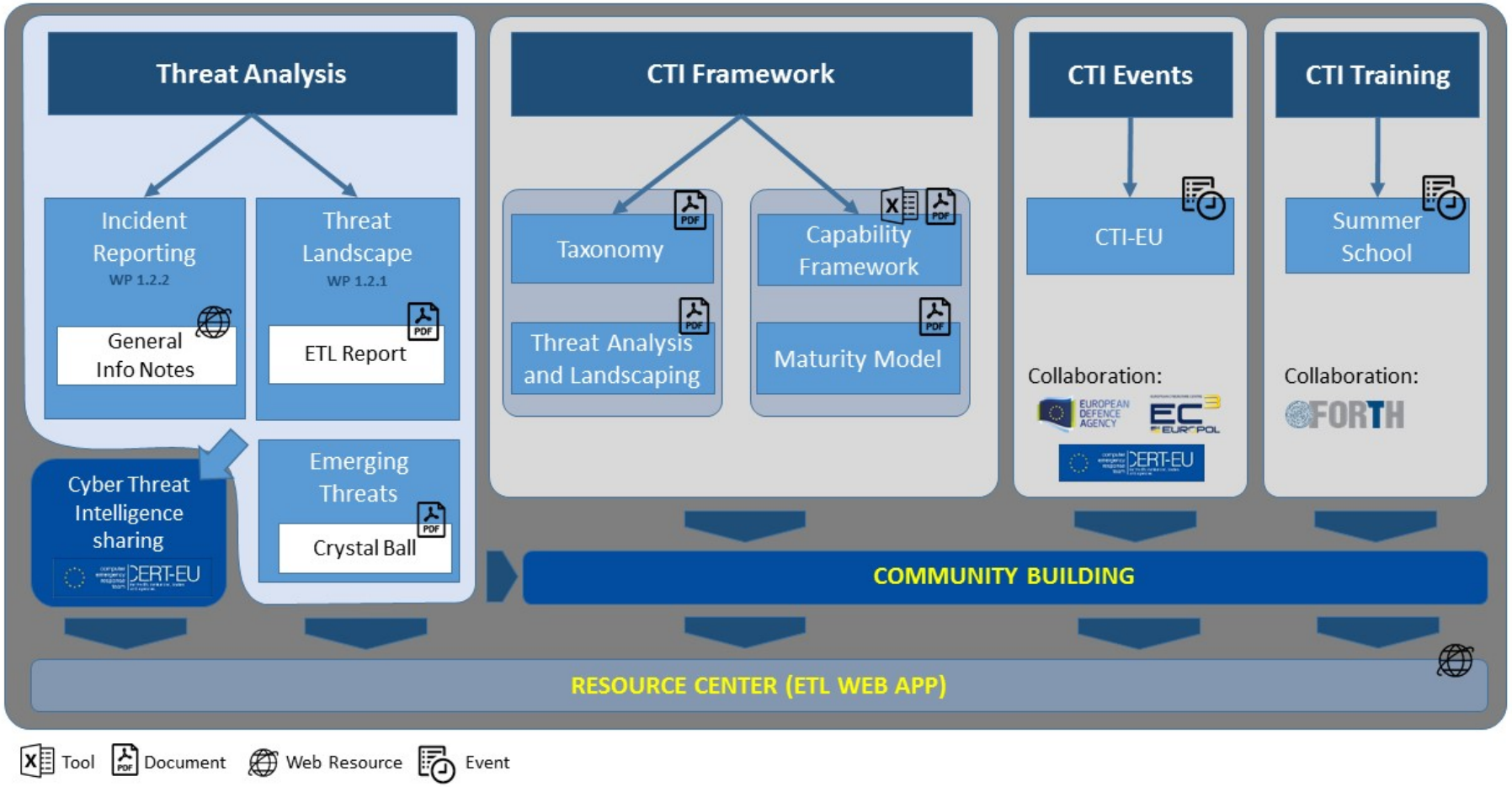
- Annual report in January
- Summary of publically available information on cyber threat information
- 139 pages of information and 664 citations
- Following an MoU worked with EC3, EDA, Cert-EU
- Report reflects an evolving landscape
- Not just a technical issue but a human issue
- Novel targeted attacks using social engineering potentially rendering sophisticated defence techniques obsolete
- Basic cybersecurity policies need to be followed at a min
- Role of management and inclusion of cybersecurity into their risk management

OUR OVERVIEW

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	⬆	2. Web Based Attacks	⬆	→
3. Web Application Attacks	⬆	3. Web Application Attacks	➲	→
4. Phishing	⬆	4. Phishing	⬆	→
5. Spam	⬆	5. Denial of Service	⬆	↑
6. Denial of Service	⬆	6. Spam	➲	↓
7. Ransomware	⬆	7. Botnets	⬆	↑
8. Botnets	⬆	8. Data Breaches	⬆	↑
9. Insider threat	➲	9. Insider Threat	⬇	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	⬆	11. Information Leakage	⬆	↑
12. Identity Theft	⬆	12. Identity Theft	⬆	→
13. Information Leakage	⬆	13. Cryptojacking	⬆	NEW
14. Exploit Kits	⬇	14. Ransomware	⬇	↓
15. Cyber Espionage	⬆	15. Cyber Espionage	⬇	→

Legend: Trends: ⬇ Declining, ➲ Stable, ⬆ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

ENISA CTI activities in a nutshell



WHAT IS ON OUR RADARS?

- Working with tools
- Looking at maturity model
- Crystal Ball: emerging trends
- Develop CTI training
- ENISA – Forth Summer School
- CTI EU

RECOMMENDED CTI LEARNING CURVE OBJECTIVES

- Understand CTI models (kill chain, OODA, Diamond Model, F3EAD, etc..)
- Understand CTI standardization
- Understand IoC Management and TIPs (e.g. MISP, IntelMQ, Maltego)
- Understand the difference to APT Landscape
- Understand Strategic CTI Reporting

(*This and more in NIS Summer School 2019*)

Thank you for your attention

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9682

info@enisa.europa.eu

www.enisa.europa.eu

SOME USEFUL URLS:

- ENISA CTI Platforms study: https://www.enisa.europa.eu/news/enisa-news/enisa-publishes-first-study-on-cyber-threat-intelligence-platforms
- ENISA Infonotes: https://www.enisa.europa.eu/publications/info-notes#c5=2008&c5=2018&c5=false&c2=infonote_publication_date&reversed=on&b_start=0
- NIS Summer School: https://nis-summer-school.enisa.europa.eu/
- ETL 2018: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
- SANS Taxonomy paper: https://www.sans.org/reading-room/whitepapers/threatintelligence/evaluation-comprehensive-taxonomies-information-technology-threats-38360
- Collection of CTI sources on requirements: https://github.com/sfakiana/FIRST-CTI-2019
- MITRE Attack Framework: https://attack.mitre.org/