CTI Capability Maturity Model

2018 CTI-EU, Brussels | November 2018

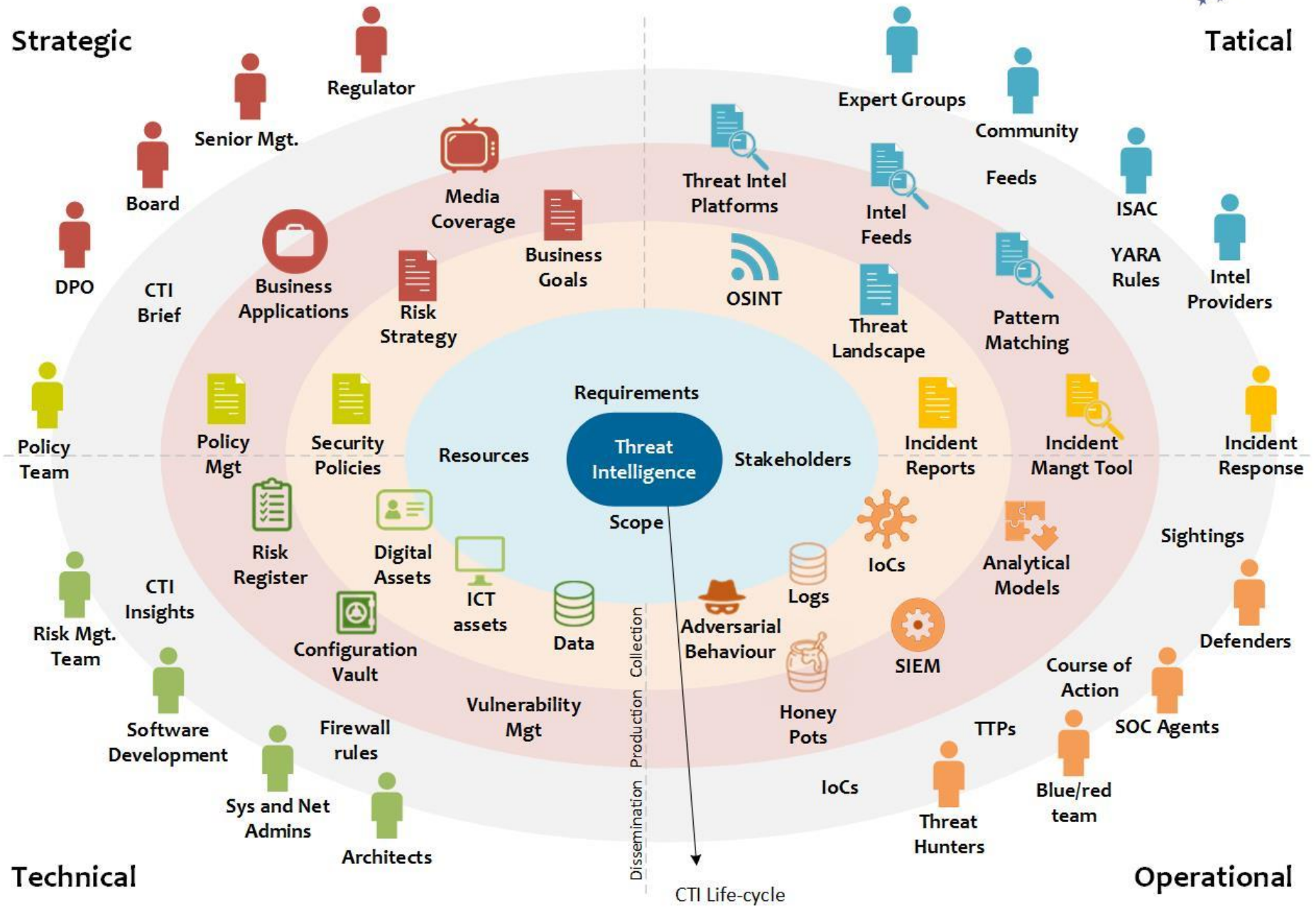
MARCO LOURENCO - ENISA Cyber Security Analyst Lead

European Union Agency for Network and Information Security

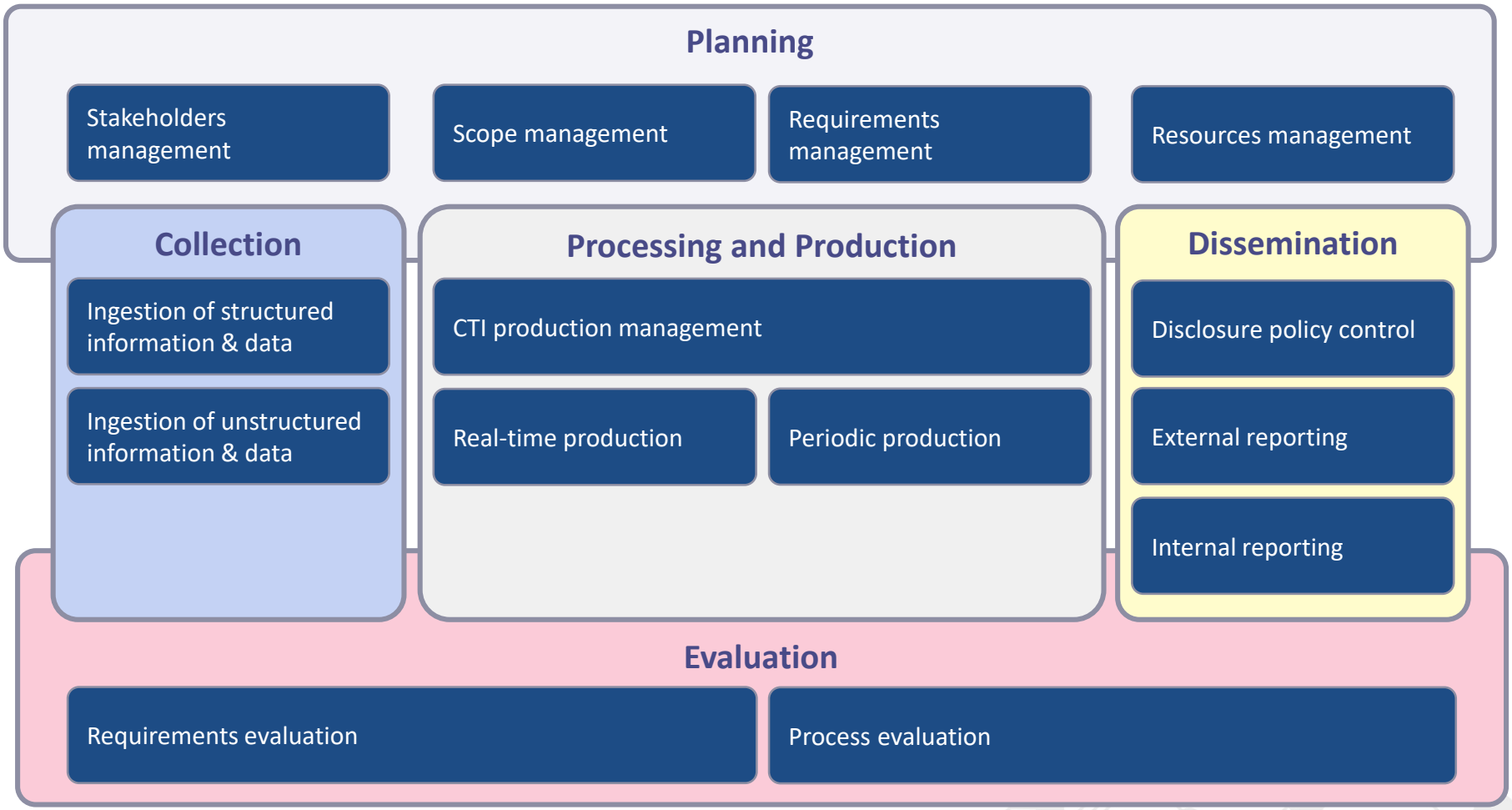
Whoami

Started as data forensics analyst for the **financial sector** during the 90s. Worked with **Interpol** in criminal investigation system projects in early 2000s. With **European External Action Service** as CISO in mid 2000s. **United Nations** and **Microsoft** as regional manager in EMEA during the last 10 years working with **government agencies** in cyber threat intelligence. Since this year in **ENISA** as cyber security analyst lead.

Cyber Threat Intelligence Model



CTI capabilities



Aligned and relevant to stakeholders and the business.

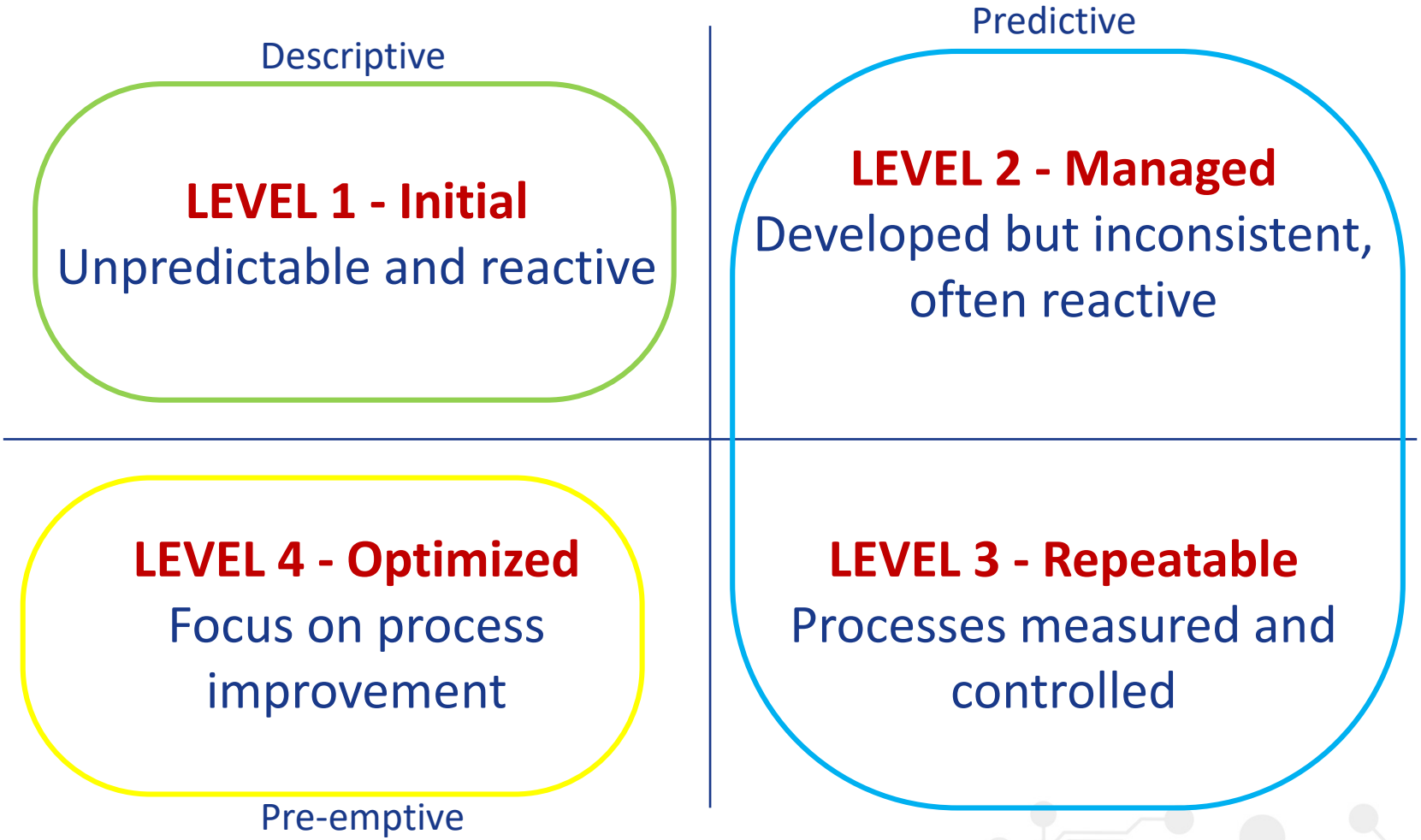
Promote a better understand of the threats targeting the organization.

Produce actionable advice that can be acted upon and influence decisions.

Promotes learning and improvement

A Model for assessing current and desired maturity state of the capabilities required to produce cyber threat intelligence.

Maturity levels



Maturity scorecard - planning

Stakeholders management | Scope management | Requirements management | Resources management

Type/level	Initial	Managed	Repeatable	Optimized
Strategic	Board and senior managers unaware of what CTI is and the team responsible for it	Board and senior managers aware, occasional CTI is offered rarely, if ever, acted upon	Threat intelligence pushed by team on big issues; board receives and considers Information	Threat intelligence a routine part of decision-making, with advice sought on all major decisions
Operational	No tasking to identify actvity-related attacks or groups who plan attacks openly	Broad tasking to identify whether attacks are occurring as a result of activities	Specific tasking to investigate a group or activity-related attack	Develop capabilities where there is indication of a return on investment
Tactical	Consumption of unstructured external information from feeds and news articles.	Regular access to threat data and information from CTI suppliers.	Correlation of external and internal threat data.	Integration of external threat data sources with SIEM.
Technical	No specific requirements for technical threat intelligence	Requirements are broad, such as consume all publically available feeds	Requirements are specific and relevant. IoCs for a specific group	Results of evaluation are an active part of requirement setting and management of the process

Maturity scorecard - collection

Ingestion of structured information & data

Ingestion of unstructured information & data

Type/level	Initial	Managed	Repeatable	Optimized
Strategic	None	Small number of sources consumed. A focus on 'overview' style articles or reading other people's analysis on the same topic	A focus on reputable, well-known sources of information in key areas.	Large range of sources, including economic, socio-political, foreign language journals, press articles, and products of other CTI types.
Operational	Attempt to analyze data from activity-related attacks	Attempts made to find an activity or event correlated to attack types	Activity-related attacks regularly predicted, but no coordinated response	Activities that result in attacks robustly understood, and appropriate monitoring in place. Response planned;
Tactical	No tactical information collected	Irregular decision making on source acquisition. Mostly open- or sources of unknown reputation	Regular decision making on source acquisition and re-alignment. Wider range of mostly reputable sources	Established procures to acquire, evaluate and re-alignment sources.
Technical	No collection	Ad-hoc collection, e.g. from occasional reports. Indicators are manually actioned, e.g. by logging onto hosts to check for registry paths or looking at firewall logs.	Collection from public feeds. Automatic searching for host-based indictors across the whole infra, probably utilising third-party software.	Collection from public feeds, and private feeds such as sharing relationships. Indicators of all types automatically searched for in network traffic and on hosts;

Maturity scorecard - production

CTI production management | Real-time production | Periodic production

Type/Level	Initial	Managed	Repeatable	Optimized
Strategic	No analysis; any sources consumed are reported directly	Some analysis of sources and verification of content of overview articles.	Analysis leading to insight that supports publically available reviews and commentary.	Deep analysis, leading to Insight. Mapped to business in a way that takes into account financial drivers, structure and intentions of the organization
Operational	No analysis, intelligence from sources is integrated directly	Advanced correlation and trends analysis. Application and database activity monitor	Some analysis of sources and verification of content of overview articles. Some attempt made to map to general businesses	Threats are proactively and strategically managed from a central register; Continuous research is proactively performed to understand known threats
Tactical	No integration of external data or information into the analysis.	Basic understanding of attack flow, actors, and tools.	Knowledgebase maintained of how a variety of campaigns that have targeted the organisation's industry functioned at each stage of attack.	Expert-level knowledge maintained on all key attack groups. User behavior and entity analysis. This includes breakdown of tools used, how key stages of the attack are executed.
Technical	No application of indicators to organization	Indicators are manually actioned by a staff member, e.g. by logging onto hosts to check for registry paths or looking at firewall logs.	Network-based indicators are automatically investigated by network devices	Indicators of all types automatically searched for in network traffic and on hosts; new indicators that become available are used to search through log data for historical signs of compromise

Maturity scorecard - evaluation

Requirements evaluation | Process evaluation

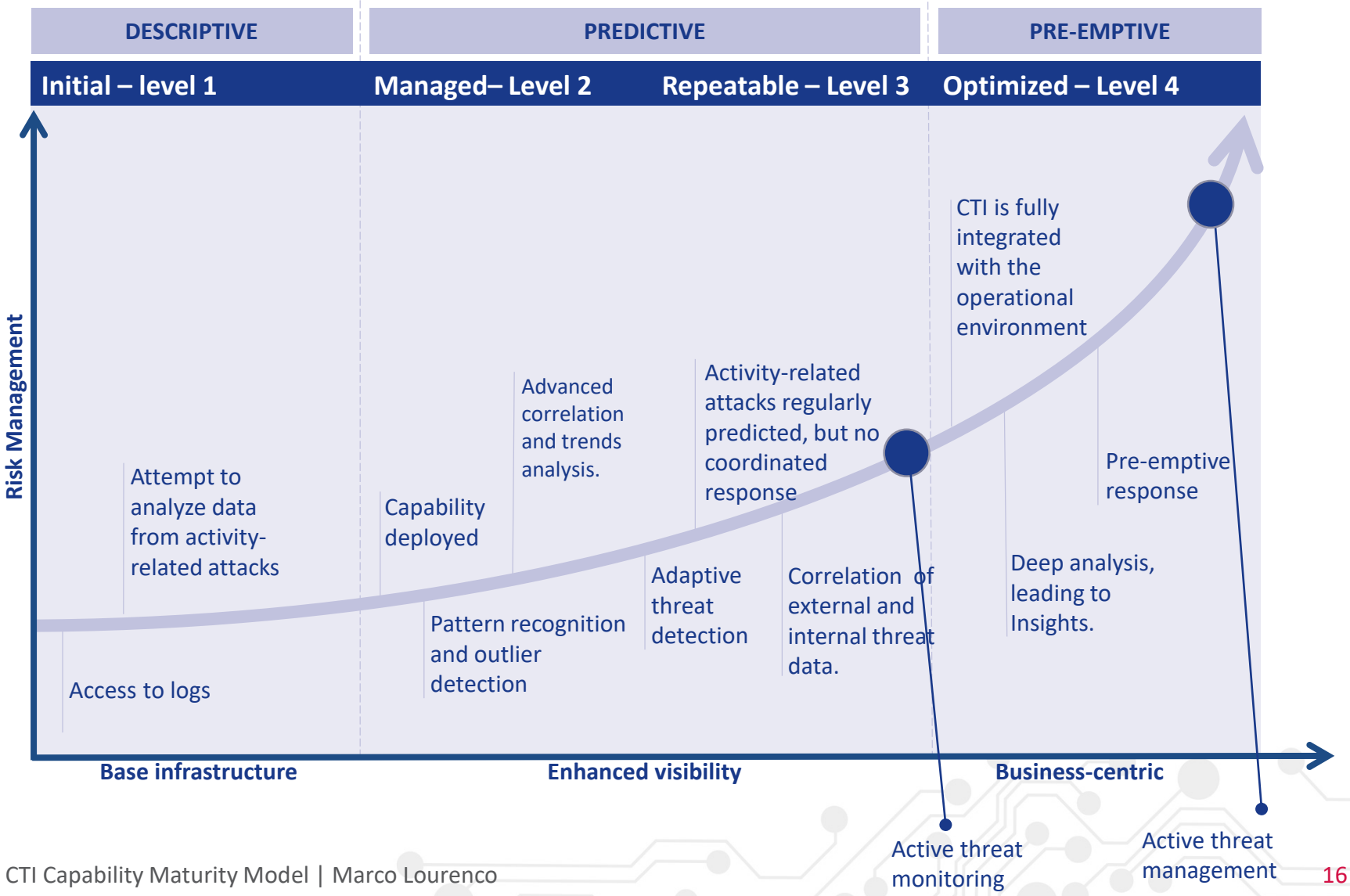
Type/Level	Initial	Managed	Repeatable	Optimized
Strategic	CTI not involved in strategic decisions	CTI considered but generally disregarded	CTI generally used in the decisions. such as increased security budget to mitigate a risk.	CTI occasionally changes decisions and regularly affects how those decisions are Implemented
Operational	No evaluation	Report prepared, identifying how many alerts were produced by operational threat intelligence and whether they were plausible	Formal process defined for evaluating the success and failure of individual cases	Efforts robustly evaluated, with undetected attacks (where detection should have been possible) subject to root cause analysis
Tactical	No evaluation	Random evaluation of the quality of CTI through a ad-hoc review process	Technical evaluation of CTI	Complete review process of the CTI
Technical	No evaluation	Monthly report prepared of how many alerts were a result of indicators from specific sources	Monthly report identifies whether verified alerts were generated as a result of an indicator that was also detected by other mechanisms	(Same as previous). Incidents that emerge are analysed to identify whether technical threat intelligence should have allowed detection sooner.

Maturity scorecard - dissemination

Disclosure policy control	External reporting	Internal reporting

Type/Level	Initial	Managed	Repeatable	Optimized
Strategic	CTI is not shared with strategic stakeholders.	Sharing with individuals at similar organisations. Board and senior managers have access to CTI but not considered as decision tool.	Reputation and trust exists on the CTI outcomes but lacks understanding on how to use it.	CTI consumed as part of decision-making, with advice sought on all major decisions.
Operational	No dissemination.	CTI is shared with operational stakeholders but no actions produced.	CTI shared with operational stakeholders and actions are taken.	CTI is fully integrated with the operational environment.
Tactical	No dissemination.	CTI is shared externally but without any specific criteria. No specific attempts to map attacker MO to organizational weaknesses	CTI is shared with specific individuals at other organisations, who would be involved in responding to an attack.	Other organisations have been successfully alerted, allowing them to better protect themselves as a result.
Technical	No dissemination.	Informal sharing with a limited audience, e.g. email	Automated sharing of verified indicators	Automated sharing of verified indicators that have been investigated

CTI maturity



Metric - Evaluating the impact of CTI

	Strategic	Operational	Tactical	Technical
Understandable				
Actionable				
Contextualized				
Sharable				
Verifiable				
Comparative				

Key takeaways

- An organization can be at different levels of maturity for the different types of CTI and capabilities;
- There is no CTI fits-all. A CTI product can meet the requirement of specific stakeholder.
- CTI is only shareable depending on the organization's disclosure policy;
- CTI can be acknowledged by certain stakeholders and actionable by others;
- Not all CTI is verifiable, depends on the resources available.
- Depending on the organization preparedness to implement certain capabilities, the decision to produce CTI internally or outsourced should be conducted as earliest as possible.

Thank you for your attention

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

louis.marinos@enisa.europa.eu

www.enisa.europa.eu