
LITTLE BOBBY
by Robert M. Lee and Jeff Haas
WE DON'T SEE ANY THREATS SO WE'RE NOT GOING TO INVEST IN SECURITY.
ARE YOU LOOKING FOR THREATS IN YOUR NETWORKS ?
NO-- WE'VE NO NEED FOR SECURITY TECHNOLOGIES.
IF YOU'RE NOT LOOKING, HOW WOULD YOU KNOW IF THREATS ARE THERE OR NOT ?
EVERYTHING SEEMS TO BE WORKING FINE !
OKAY-- SO FAITH, JUST SAY BLIND FAITH.
HAAS

CTI Capability Maturity Model

Cyber Threat Intelligence Course

NIS Summer School 2018, Crete | October 2018

MARCO LOURENCO - ENISA Cyber Security Analyst Lead

European Union Agency for Network and Information Security

Agenda

1. Whoami
2. Recapping
3. CTI capability Framework
4. CTI maturity Model
5. Good practices of CTI capability according to organizations
6. Manage the level of expectation/fulfillment KPI/Metrics
7. MedX Case Study
8. Q&A

Whoami

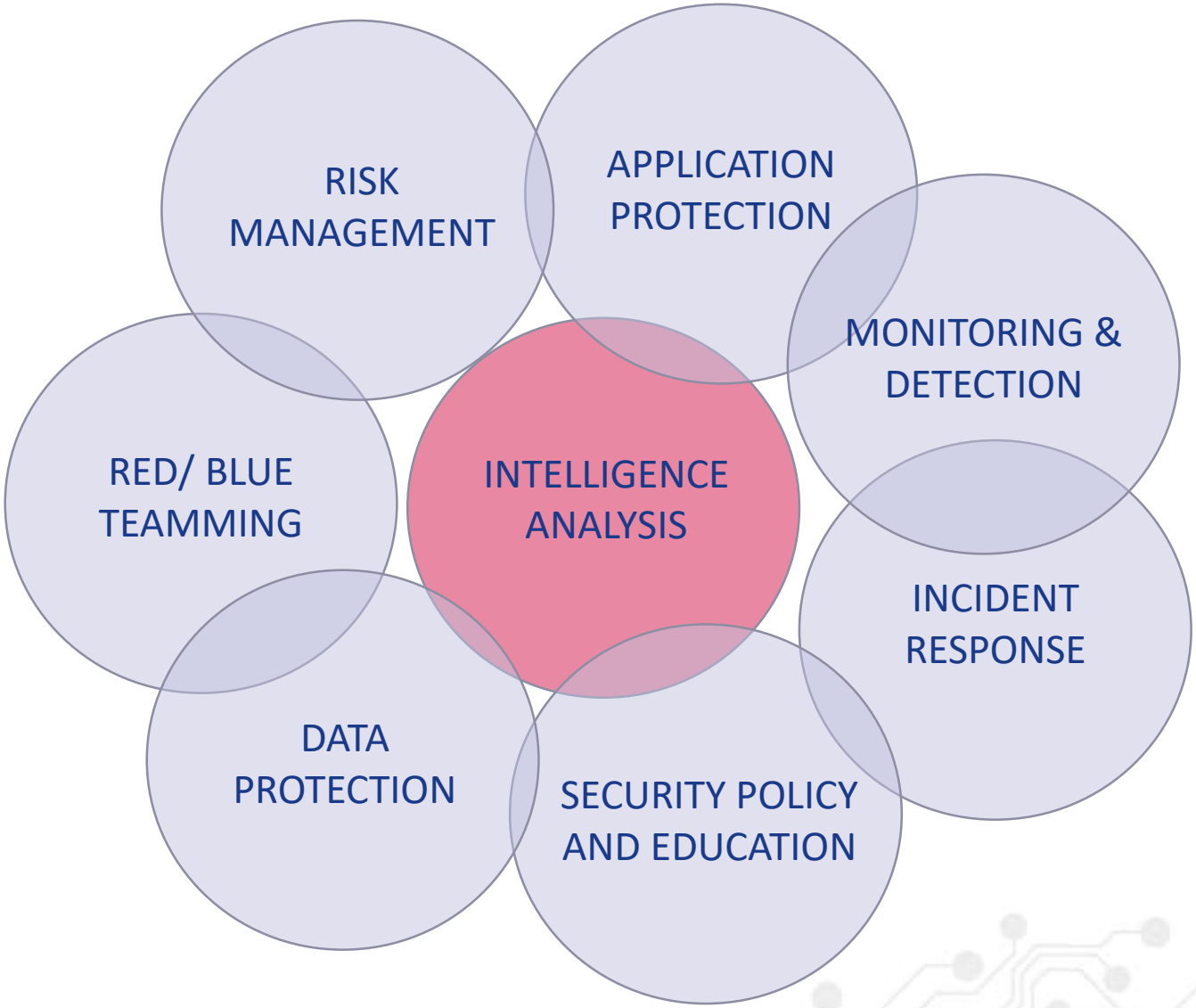
Started as data forensics analyst for the **financial sector** during the 90s. Worked with **Interpol** in criminal investigation system projects in early 2000s. With **European External Action Service** as CISO in mid 2000s. **United Nations** and **Microsoft** as regional manager in EMEA during the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

Whoami

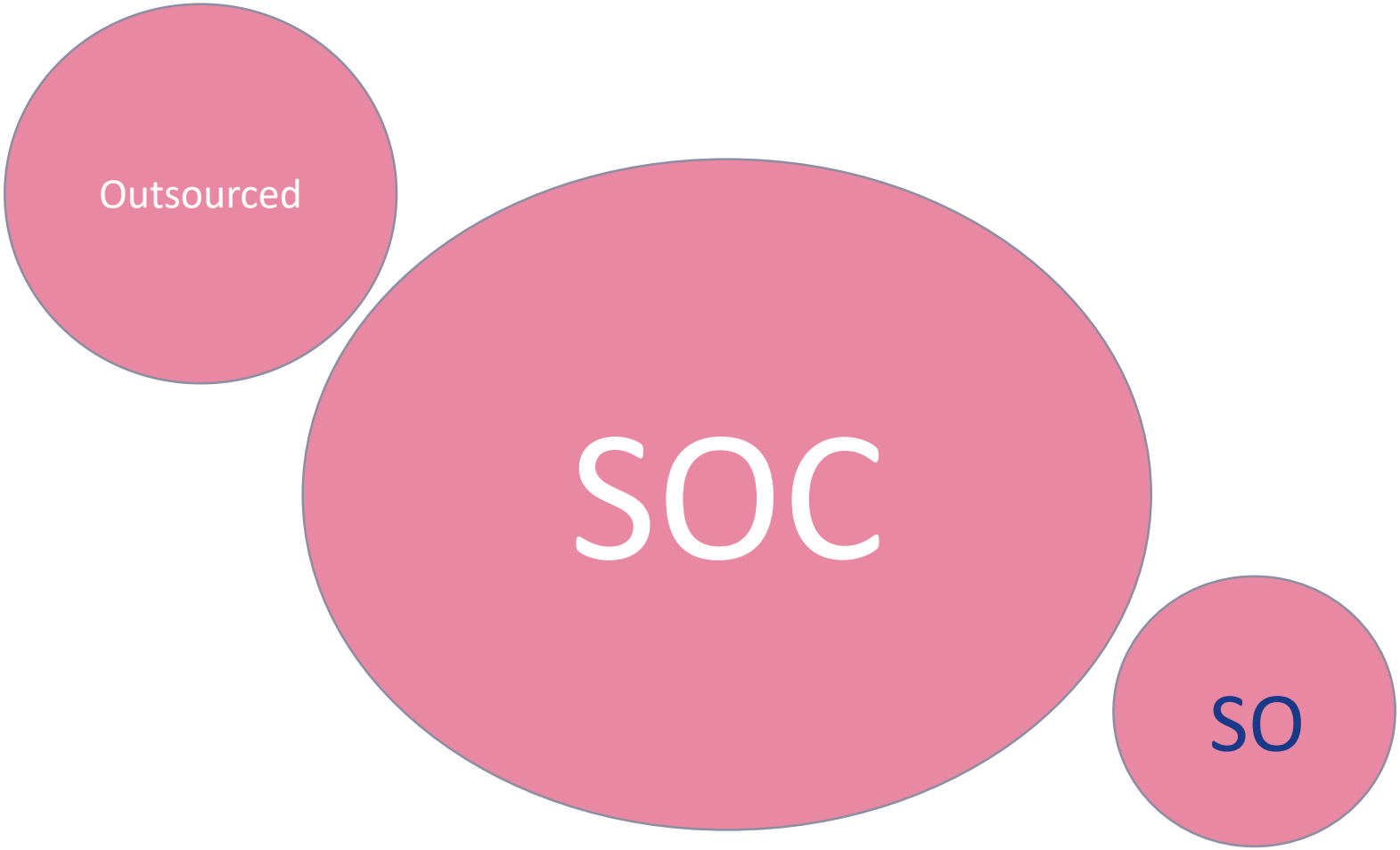
- Analyst background
  - Computer forensics
  - Criminal investigation
  - Infosec operational
  - CTIA Manager
- Threat Intelligence Analysis evangelist


STOP
IF GATE HAS
STARTED TO CLOSE
PLEASE ALLOW
THE CYCLE TO
COMPLETE

Where Analyst sit?



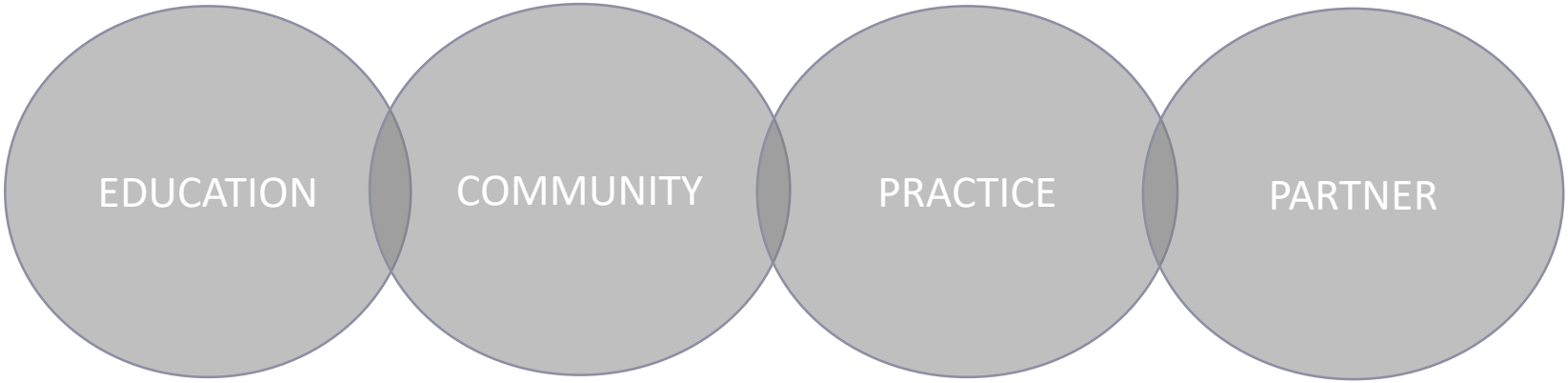
Where Analyst sit?



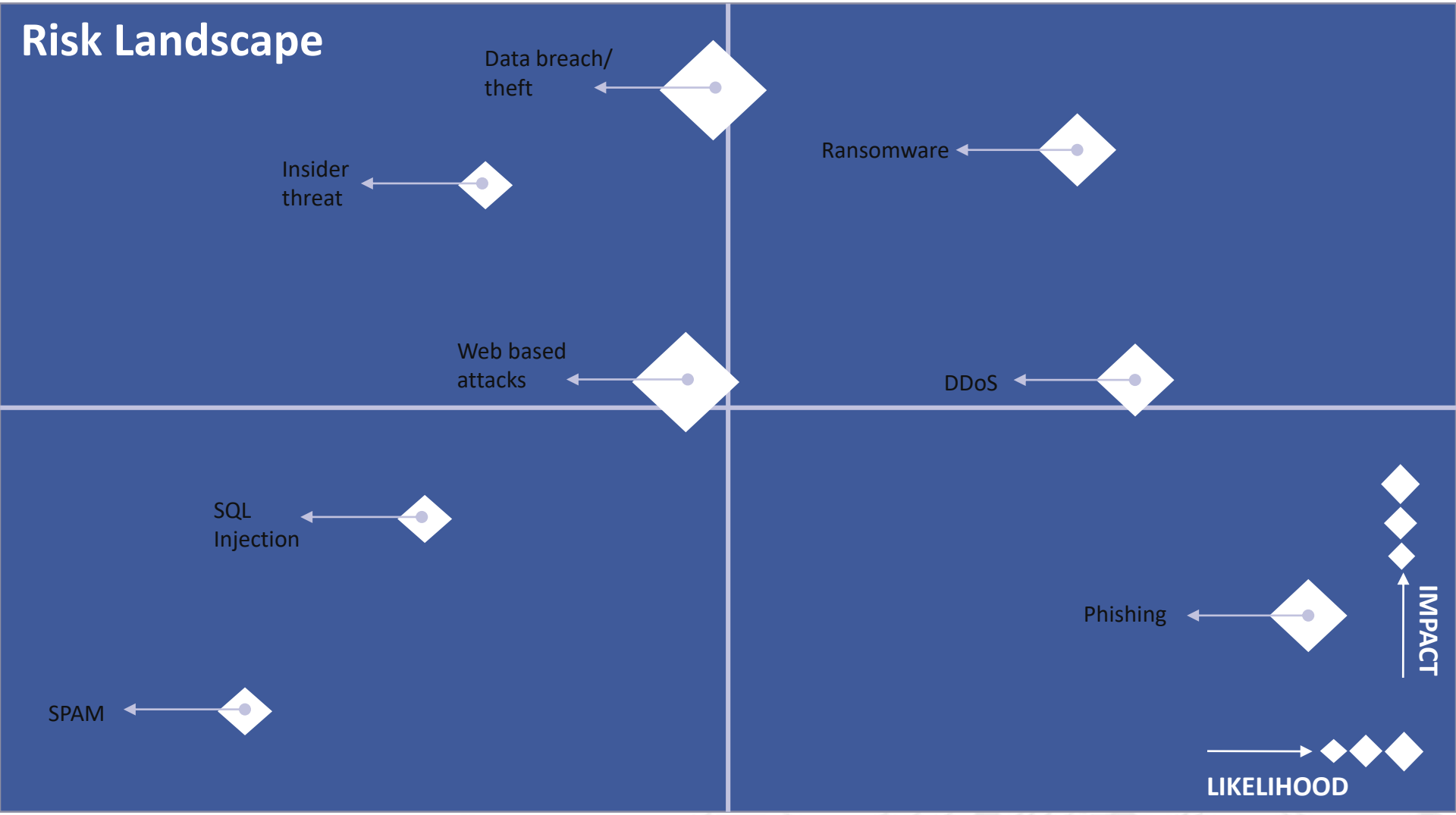
Why Cyber Threat Intelligence Analysis became an important cyber security domain?

- The urgent need for moving from reactive to proactive approach;
- Difficulties in having a better understanding of the threat landscape;
- The need for clarity and interpretation from all the data and information available;
- Going beyond what is available within the organization radar and play in anticipation;
- Profiling adversaries through behavior and attribution and get a better understanding of their intentions;
- Apply a methodological approach on how to deal with threats.

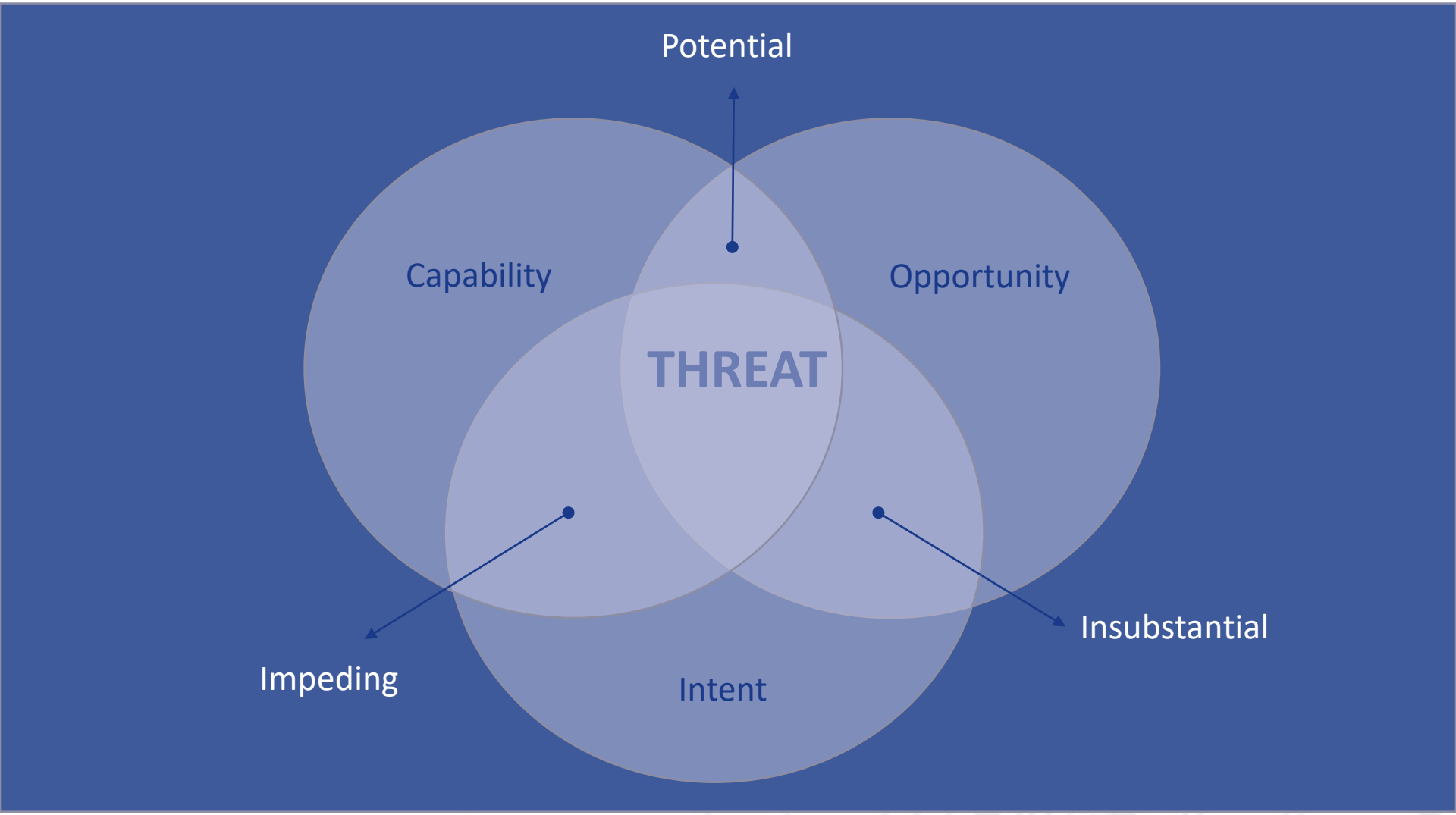
Where we need to focus?



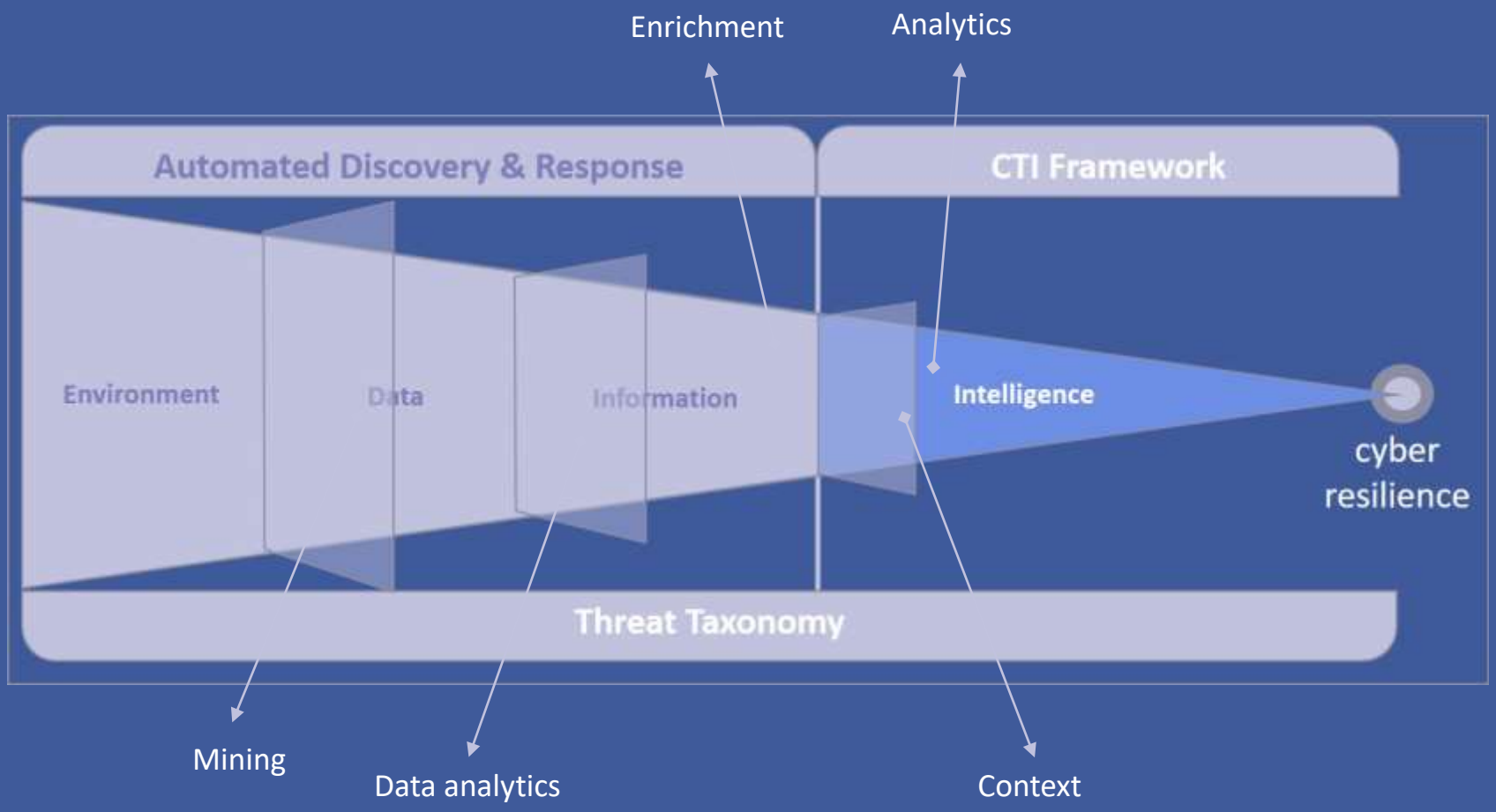
“Recapping”


Risk Landscape
Data breach/ theft
Insider threat
Ransomware
Web based attacks
DDoS
SQL Injection
Phishing
SPAM
IMPACT
LIKELIHOOD

“Recapping”


Potential
Capability
Opportunity
THREAT
Impeding
Intent
Insubstantial

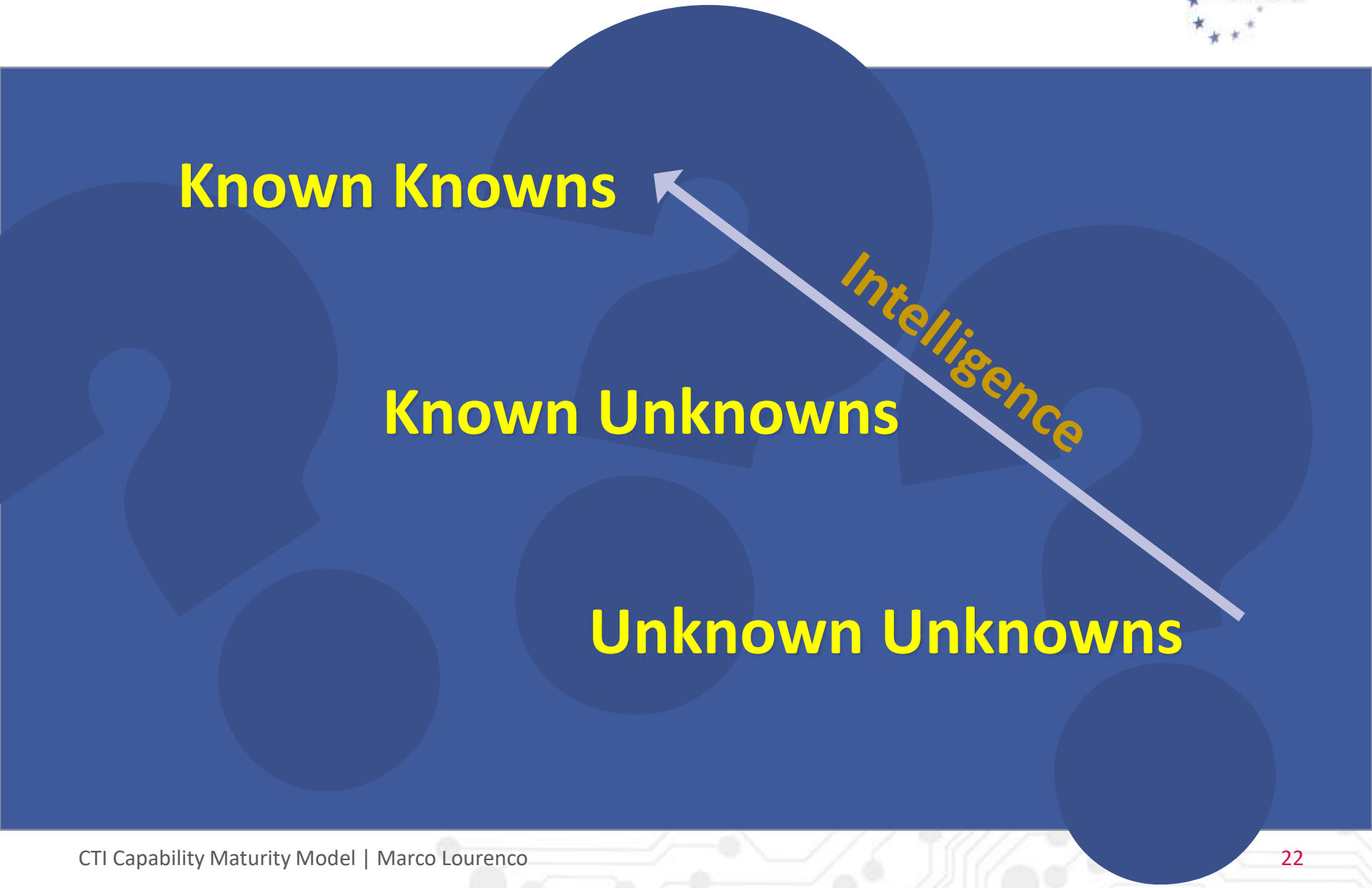
“Recapping”


Enrichment
Analytics
Automated Discovery & Response
CTI Framework
Environment
Data
Information
Intelligence
cyber resilience
Threat Taxonomy
Mining
Data analytics
Context

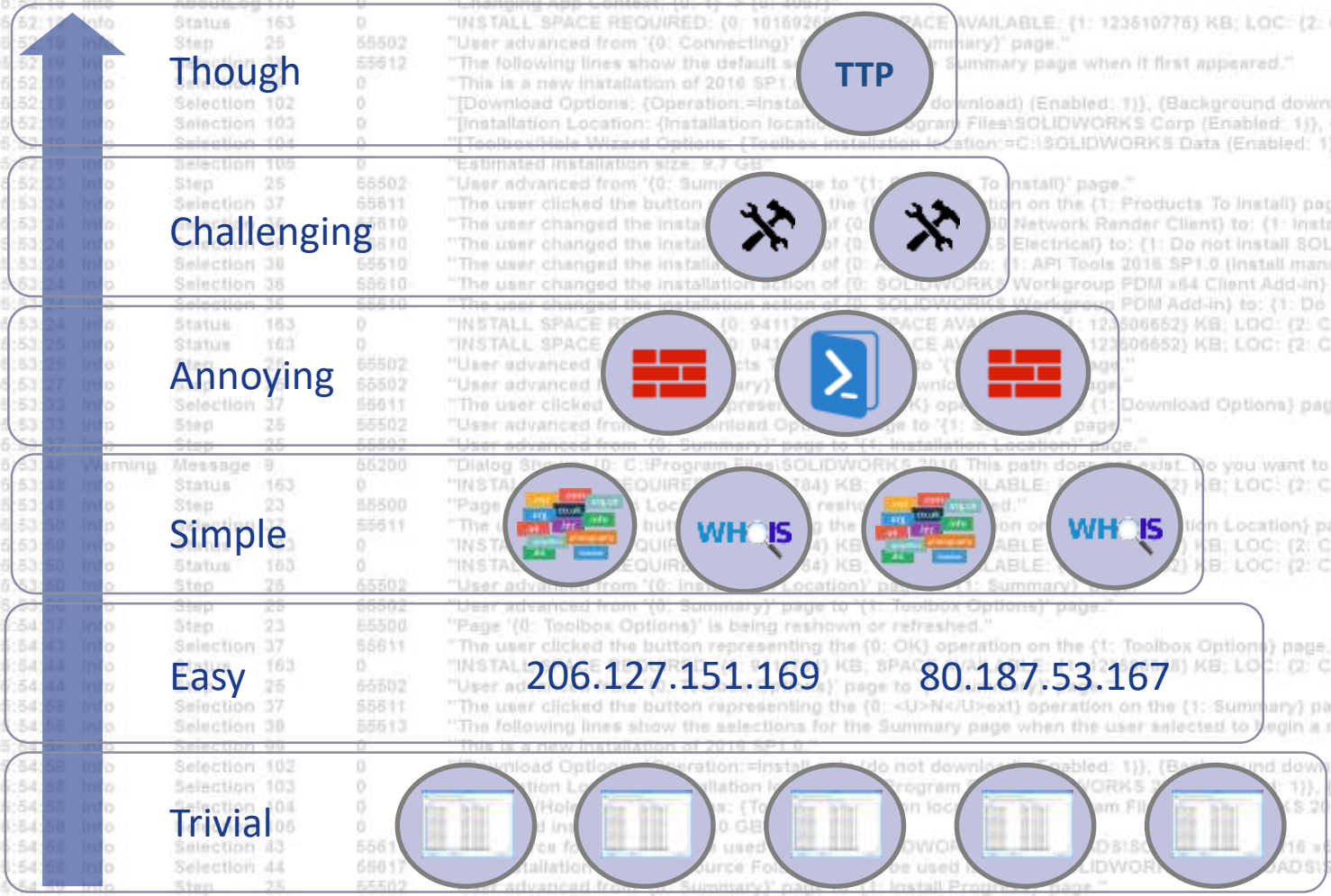
“Recapping”

“Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to conduct informed decisions regarding the subject’s response to that menace or hazard.”

“Recapping”

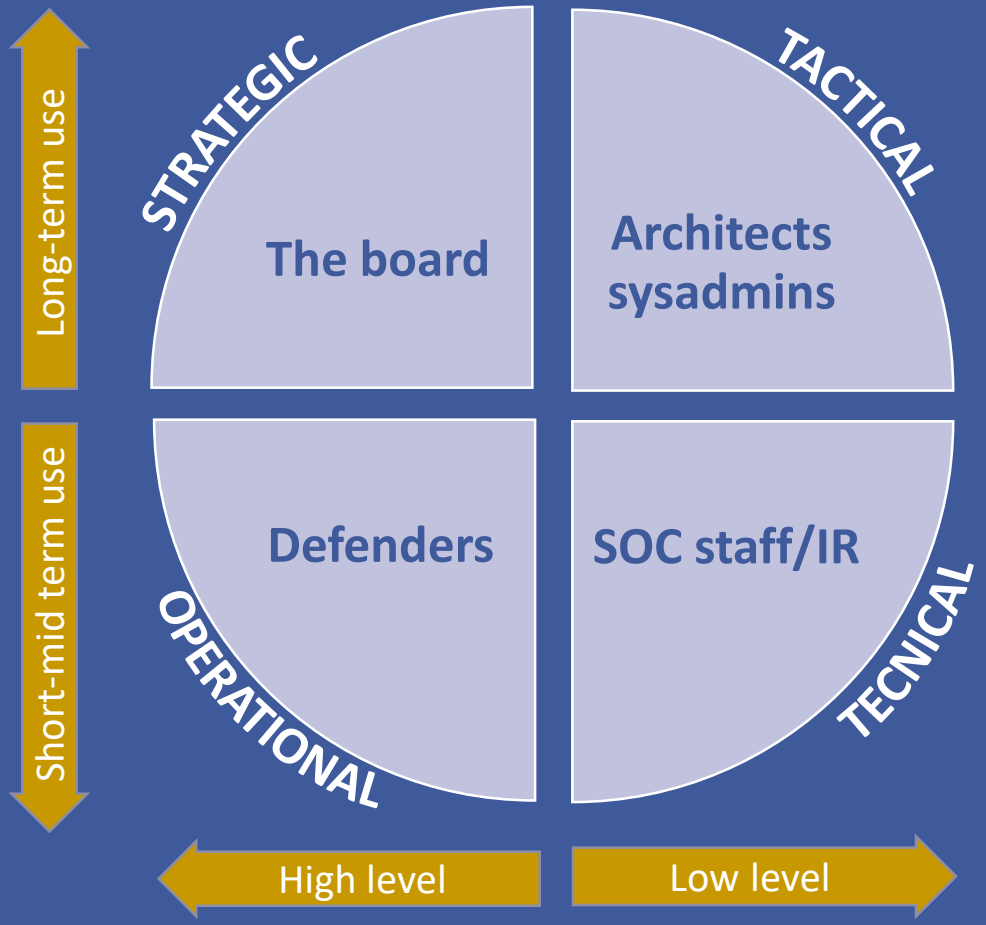

Known Knowns
Known Unknowns
Unknown Unknowns
Intelligence

“Recapping”



David Bianco - Pyramid of Pain

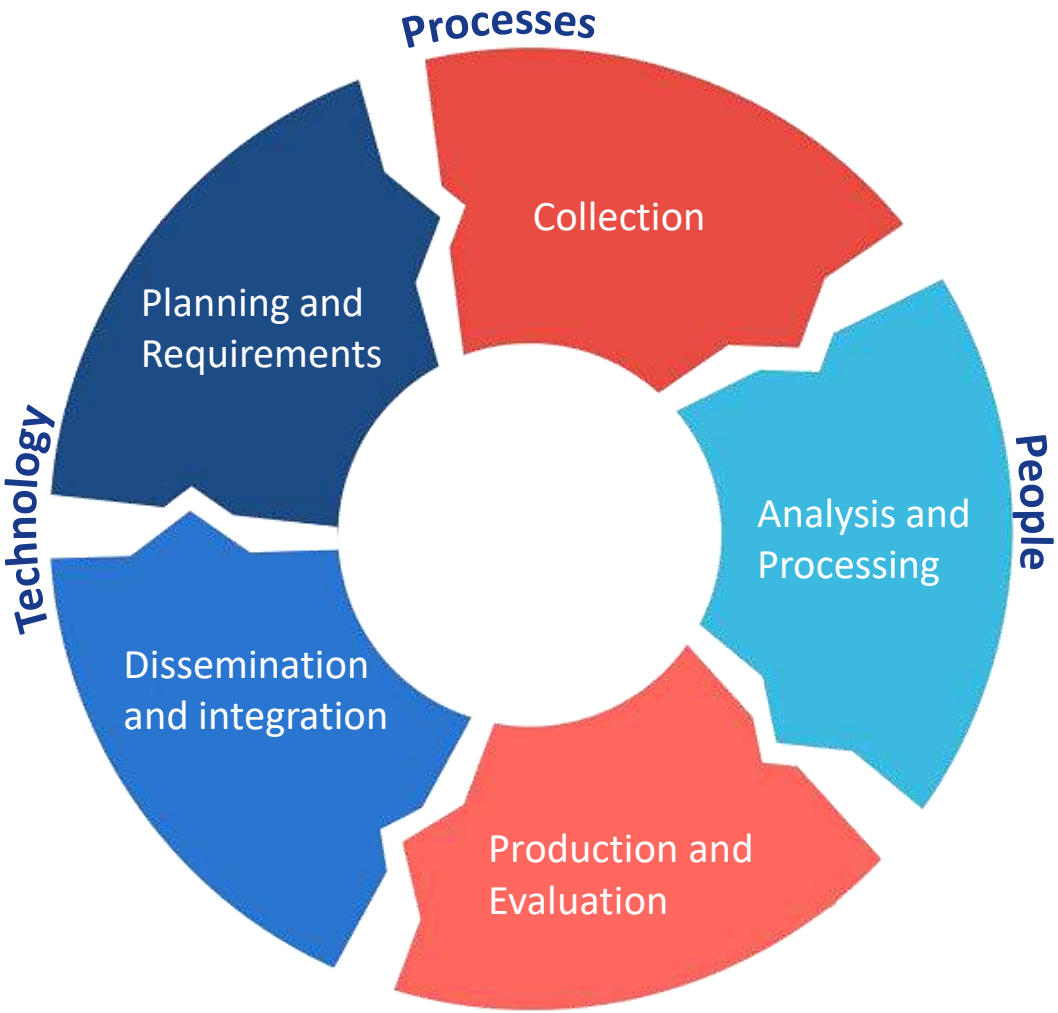
“Recapping”

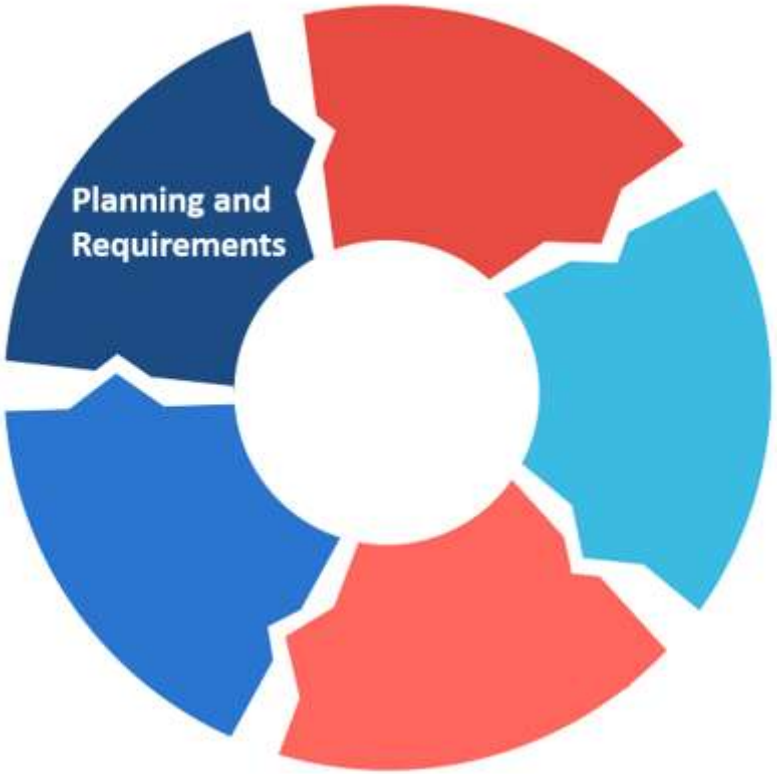

Long-term use
Short-mid term use
STRATEGIC
TACTICAL
OPERATIONAL
TECNICAL
The board
Architects sysadmins
Defenders
SOC staff/IR
High level
Low level

“Recapping”

TYPE	LEVEL	SCOPE	MAIN TASK
Strategic	High	Medium to Long Term	High Level Information for Risk Reduction
Operational	High	Short to Medium Term	Details of Specific Incoming Attacks
Tactical	Low	Medium to Long Term	Attackers Methodologies, Tools and Tactics
Technical	Low	Short to Medium Term	Indicators of Specific Malware

CTI Capability Framework




Planning and
Requirements

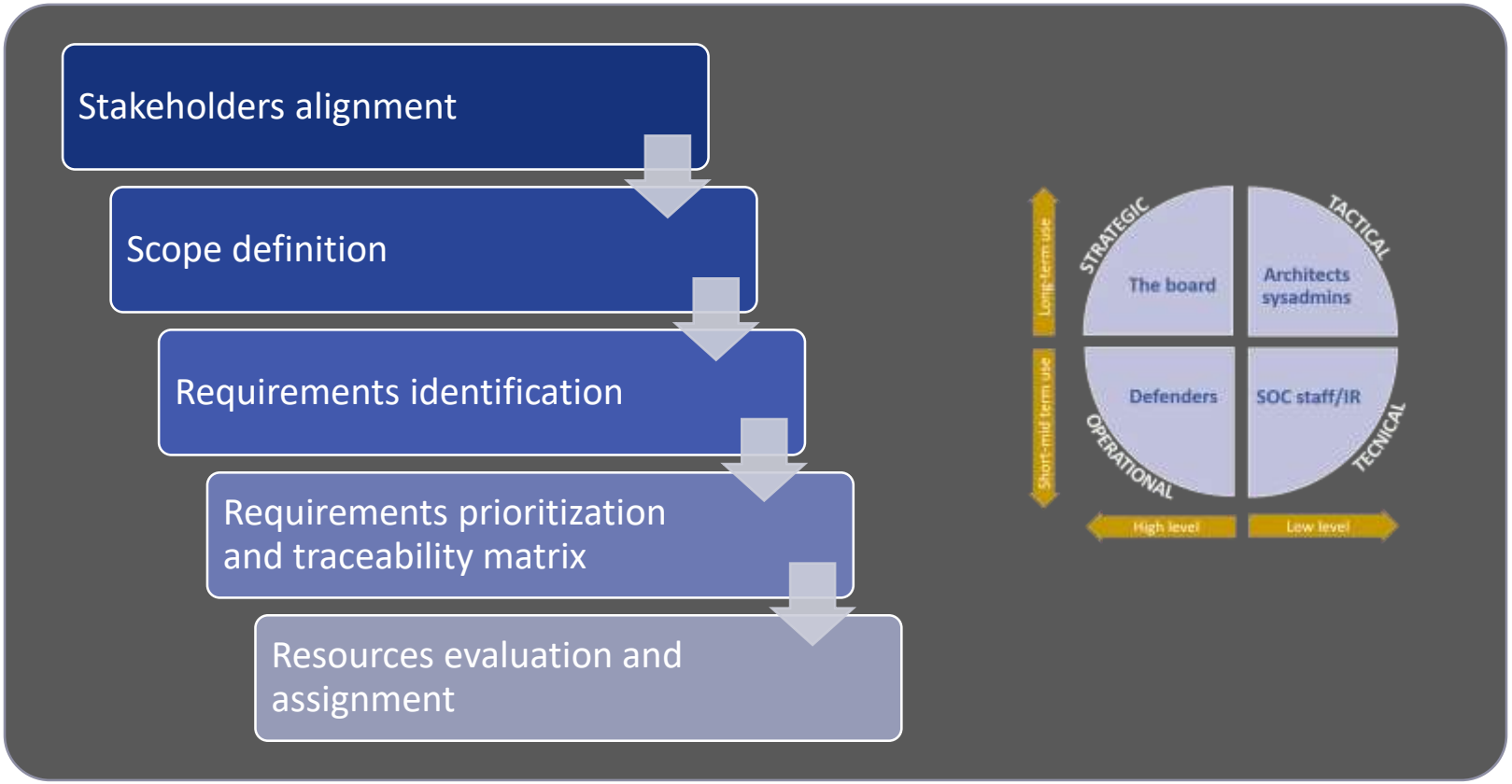
“

Failing to plan is planning to fail.

”

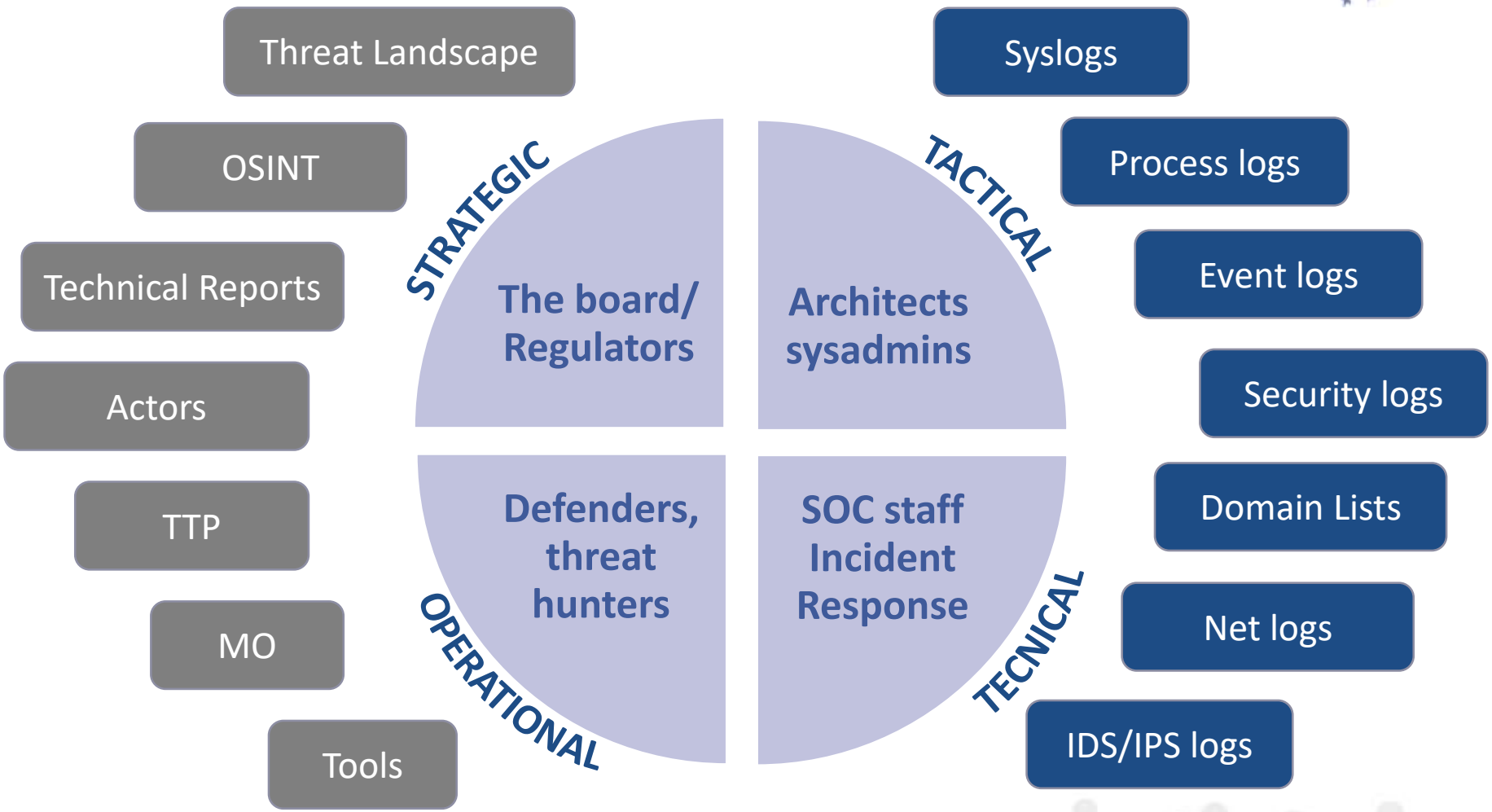
Winston Churchill

Planning


Stakeholders alignment
Scope definition
Requirements identification
Requirements prioritization and traceability matrix
Resources evaluation and assignment
STRATEGIC
TACTICAL
OPERATIONAL
TECNICAL
The board
Architects sysadmins
Defenders
SOC staff/IR
Long-term use
Short-mid term use
High level
Low level


Collection
Planning and Requirements

Collection



Stakeholders and information collection

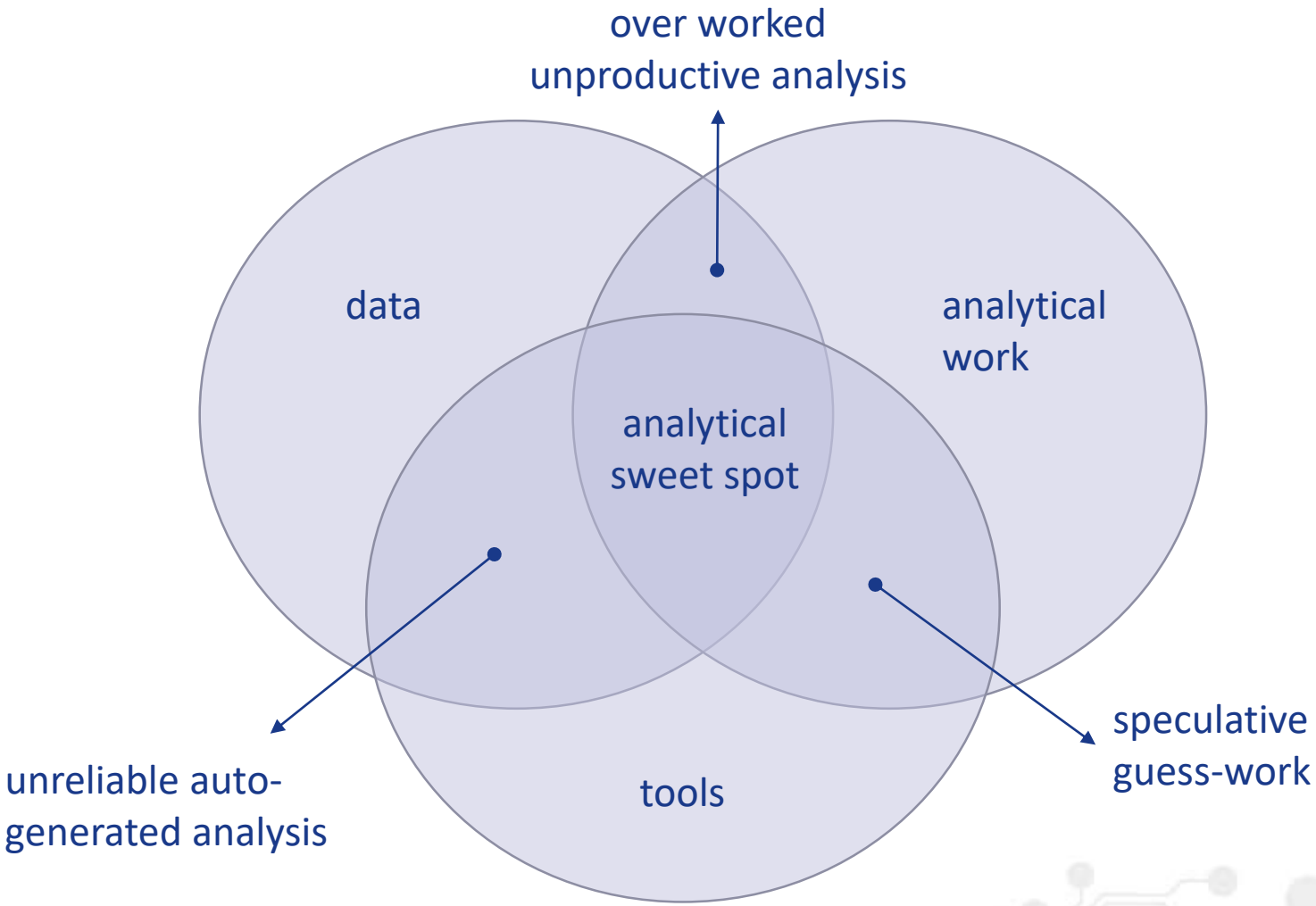
Collection

Collection Management Example

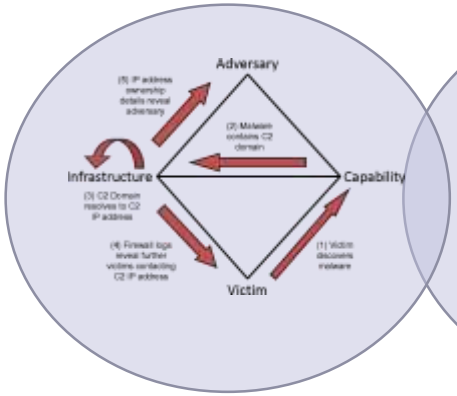
	Endpoint Protection Systems	Operating Systems	Network	Firewall
Data Type	System Alert	Host Based Logs	Netflow	System Alert
Kill Chain Coverage	Exploitation & Installation	Exploitation Installation and Actions on Objectives	Internal Reconnaissance, delivery and C2	Internal, Reconnaissance, Deliver and C2
Follow on Collection	Malware sample	Files and timelines	Packet capture	Netflow
Typical Storage in Days	30 days	60 days	23 days	60 days


Collection
Planning and Requirements
Analysis and Processing

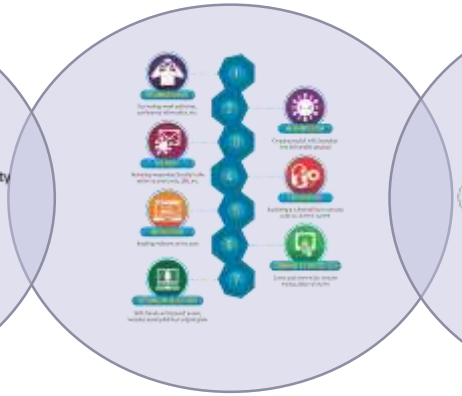
Analysis and processing



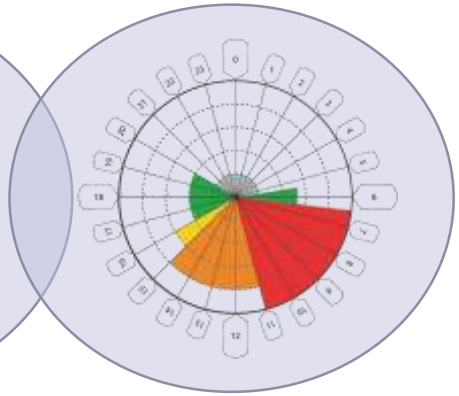
Analysis and processing



Diamond Model of Intrusion Analysis



KILL-CHAIN Lockheed Martin

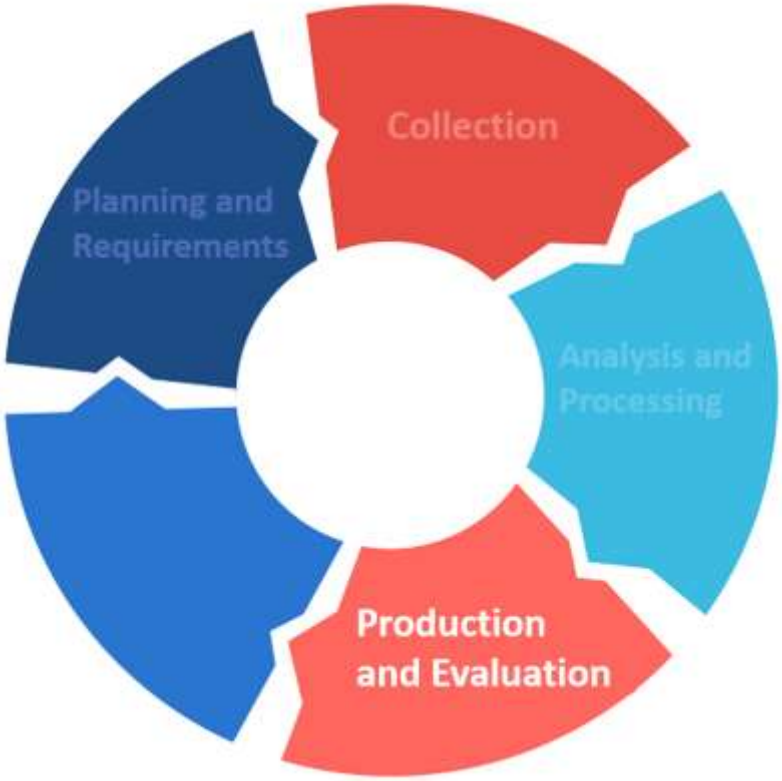


Campaigns Heat Map

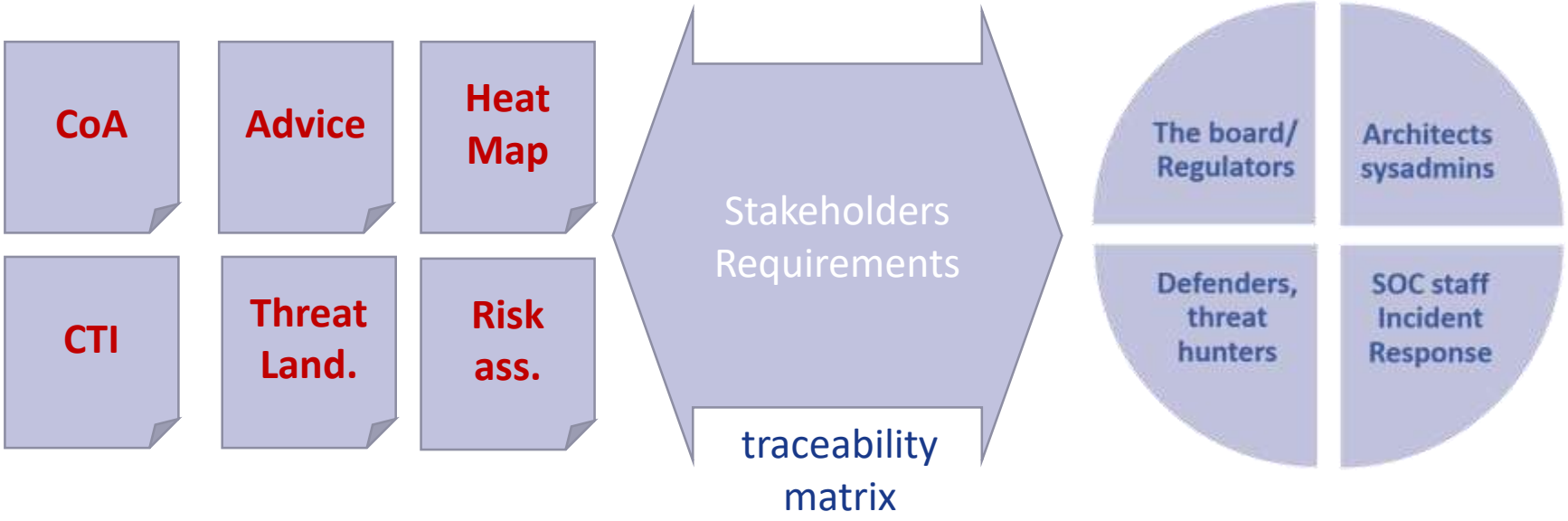
TIP

Threat Intelligence Platforms

Excel


Collection
Analysis and Processing
Production and Evaluation
Planning and Requirements

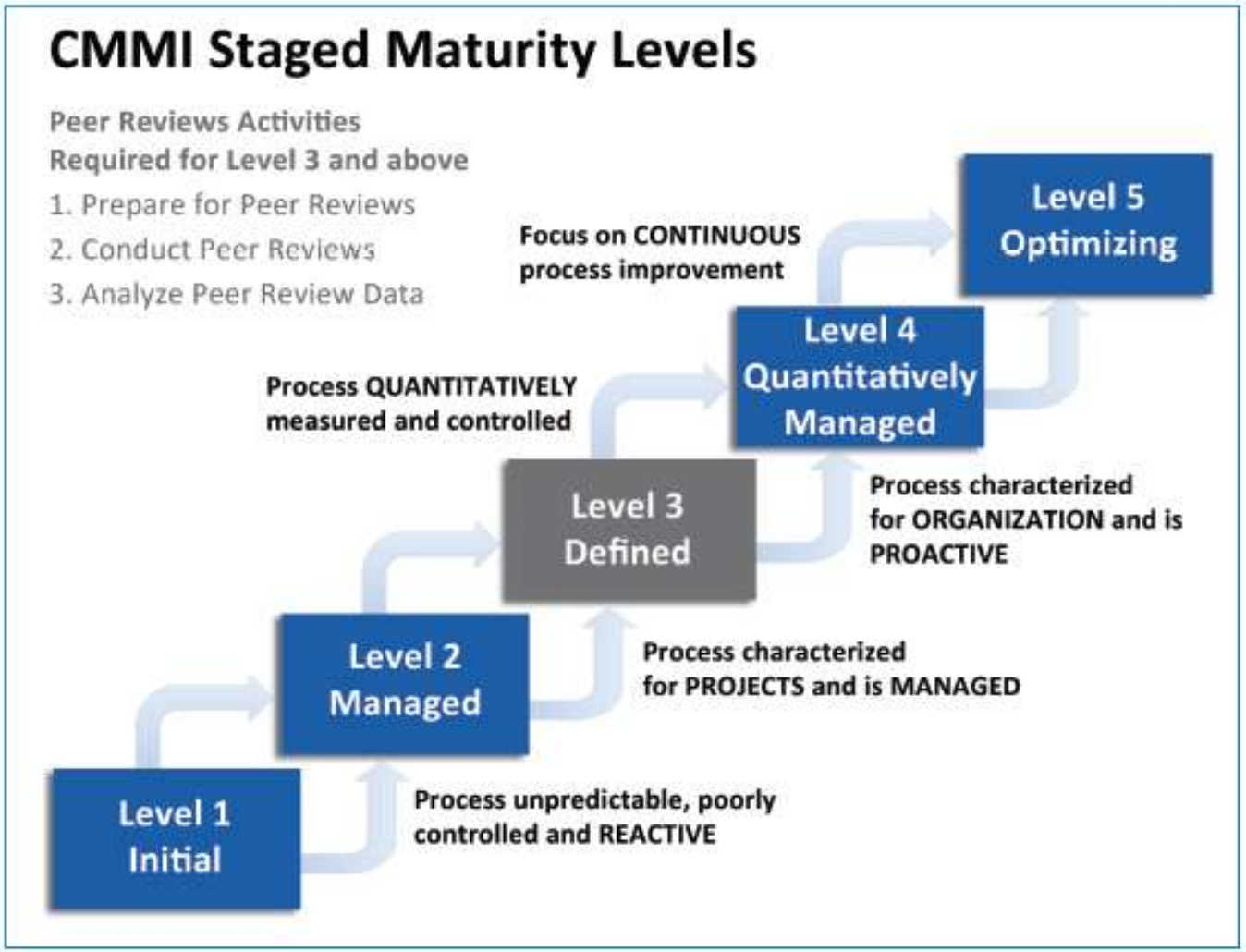
Production and evaluation



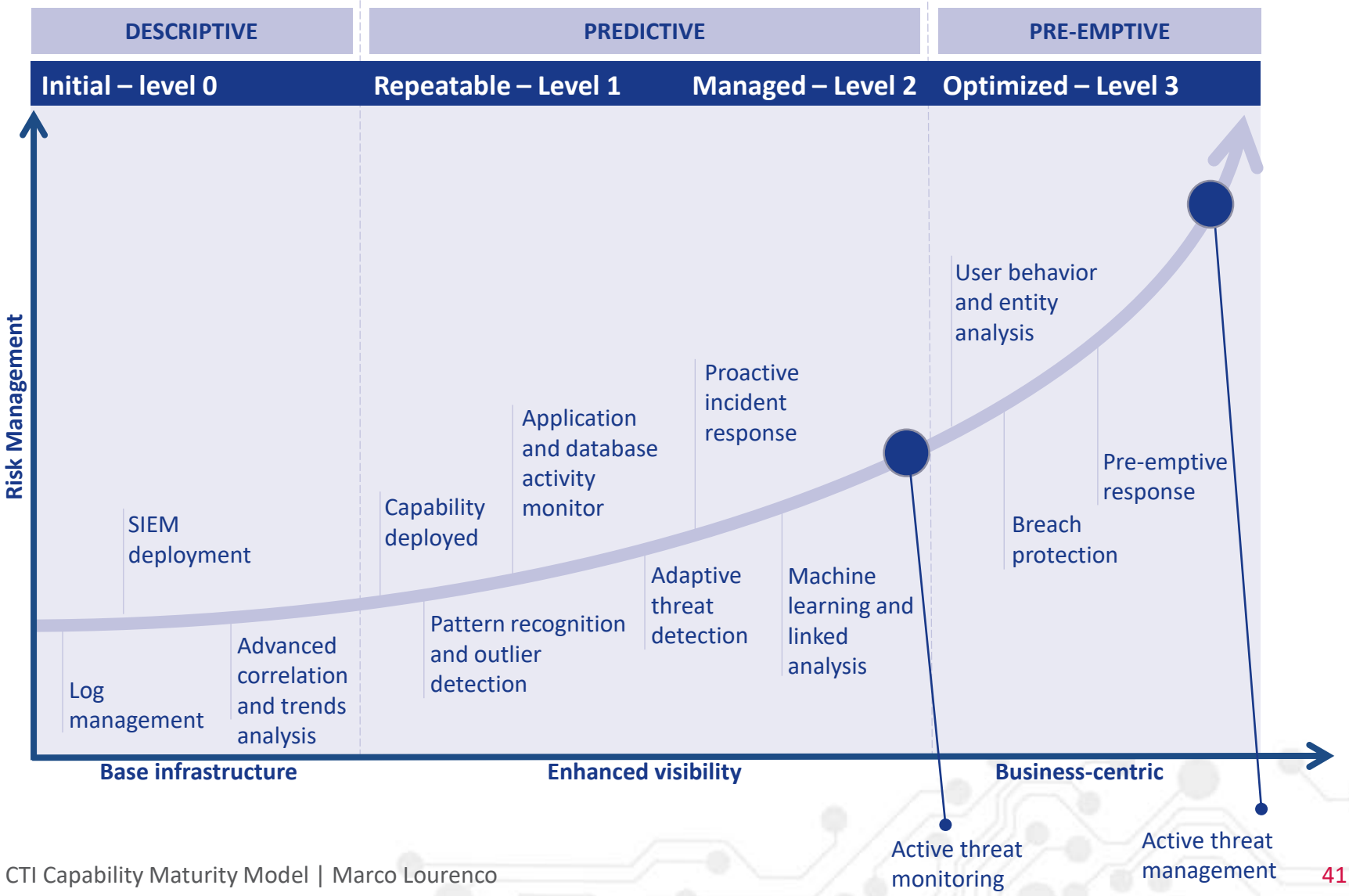

Collection
Analysis and Processing
Production and Evaluation
Dissemination and integration
Planning and Requirements

Dissemination and Integration

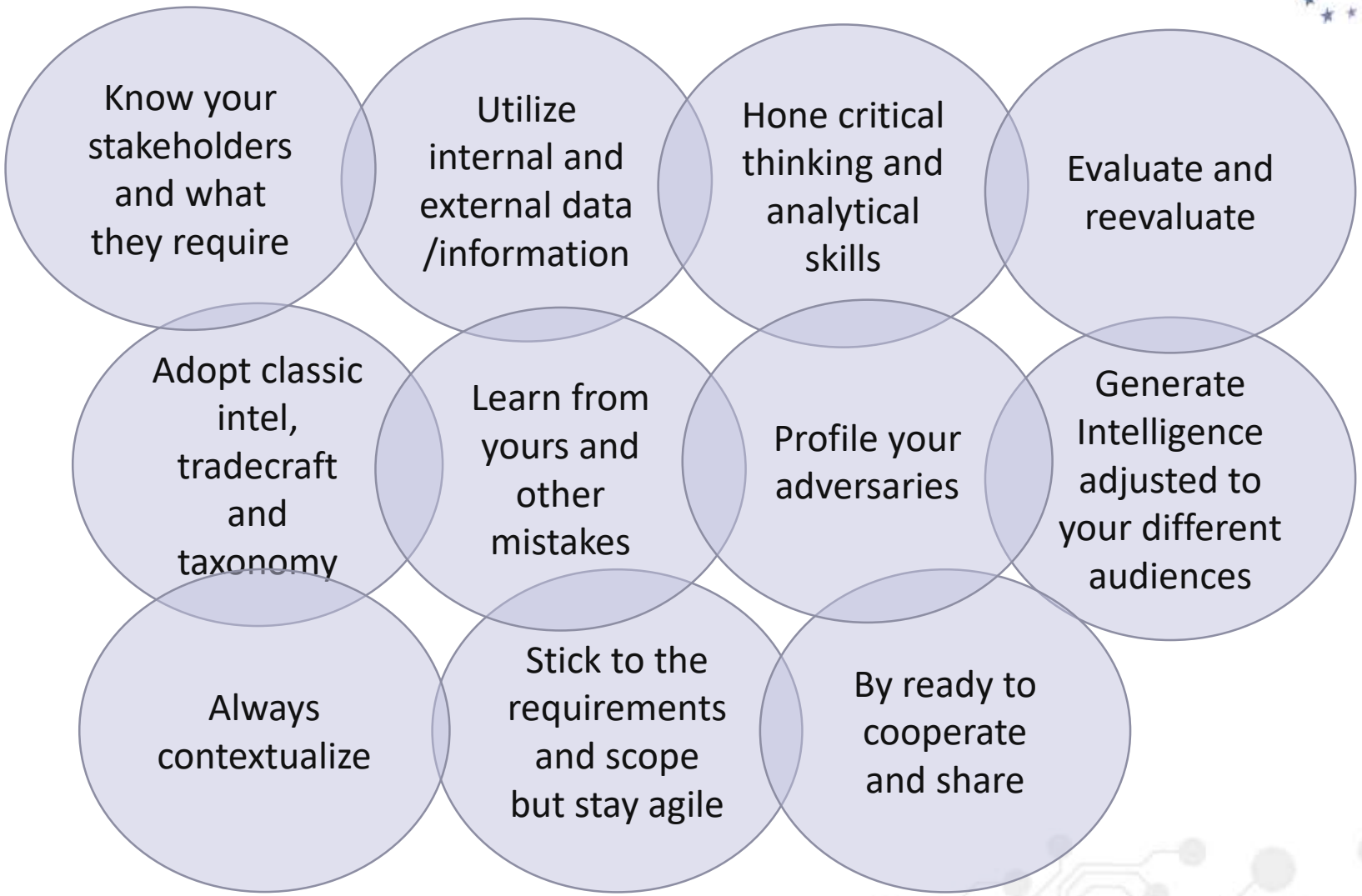
Maturity Model



CTI maturity



Good practices



2018 CTI-EU Bonding

Getting the Cyber Threat Intelligence Community together

https://www.enisa.europa.eu/2018-cti-eu-event/enisa-cti-eu-event

Brussels, 5 and 6 November 2018

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