2024
FIRST
Cyber Threat Intelligence Conference

Berlin, Germany
April 15-17, 2024

Blueprint for Maturity: Crafting a Tailored Cyber Threat Intelligence Maturity Model

Kiraga Sławek
16.04.2024

Agenda

1. Maturity models unpacked: Why bother?
2. “But the intelligence is such a complex field…”: Structuring the Unstructured
3. Making the Intangible Tangible: Turning Ideas into Action
4. DIY CTI: Make your own plan for maturity

How did it all begin?

My expierience a.k.a whoami

Different shades of intelligence for:

- Governmental Stakeholders
- Pharmaceutical Industry
- Banking & Finance

What are maturity models? Why do we need them?

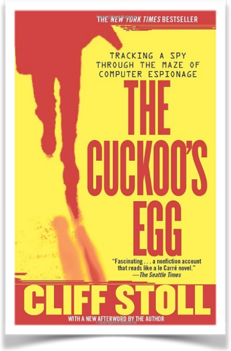
CMMI Capability Maturity Model Integration

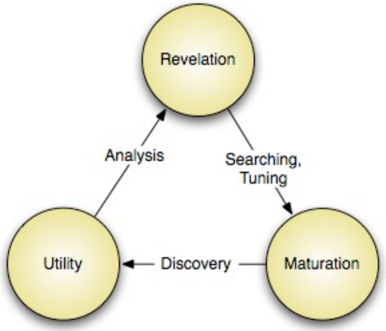
ITIL® Maturity Model

PMI Project Management Institute

- Logical sequence of levels or stages, from initial state to maturity
- Predictable patterns of evolution
- Levels presented by actionable details
- Self-assessment and benchmarking
- Guided growth and development
- Improved efficiency and effectiveness

How CTI may mature…if left alone


THE NEW YORK TIMES BESTSELLER
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE
THE CUCKOO'S EGG
"Fascinating . . . a nonfiction account that reads like a le Carré novel." —The Seattle Times
CLIFF STOLL
WITH A NEW AFTERWORD BY THE AUTHOR



Security Awareness

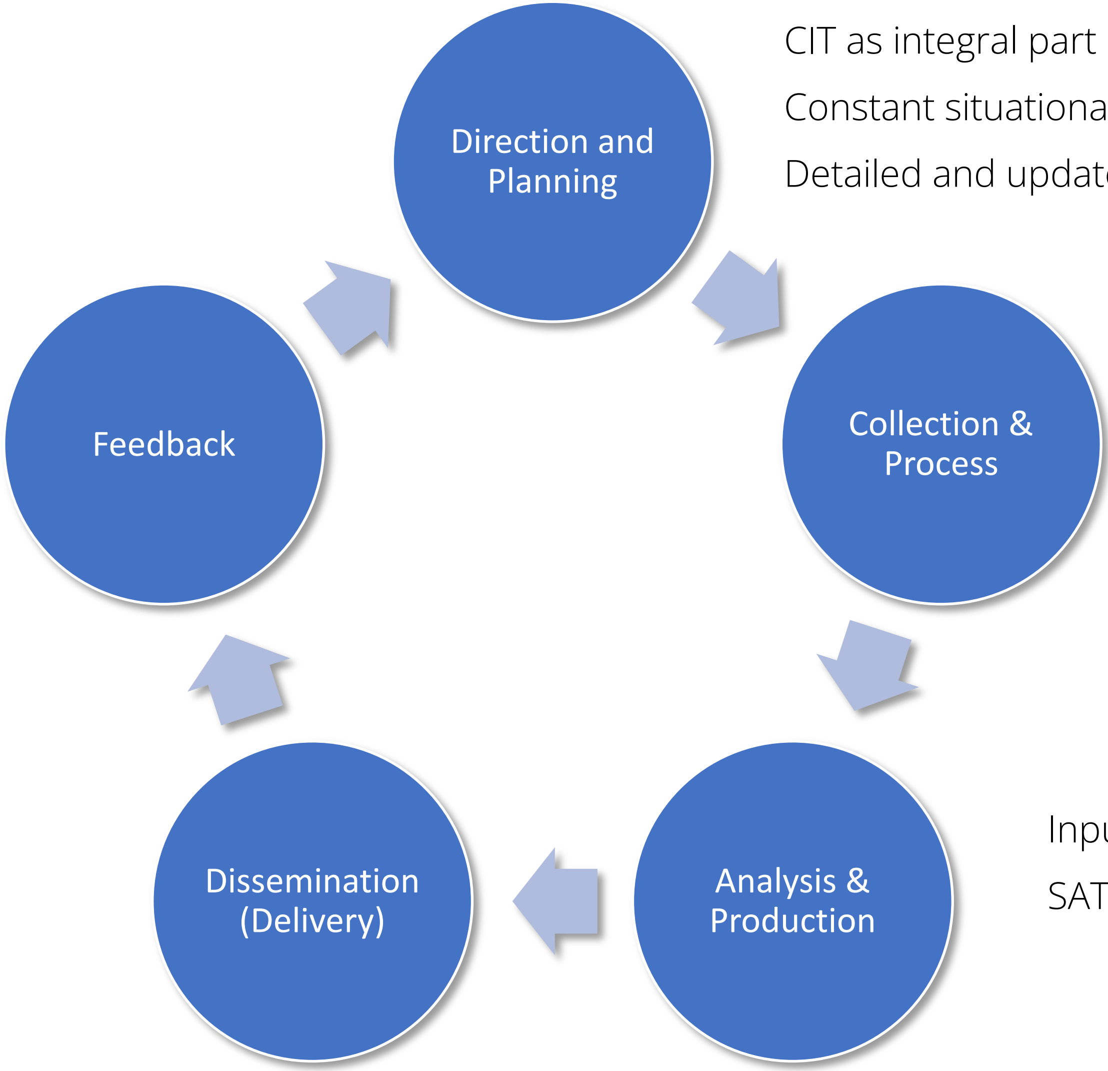
OT / ICS

Threat Hunting

Red Team

Senior Leaders

What is a mature CTI?



CIT as integral part of the organization

Constant situational awareness

Detailed and updated requirements

Collection Management Framework

Tools & Automatization

Input -> Process – Output

SAT & Bias Management

Recipients: Tools & Humans

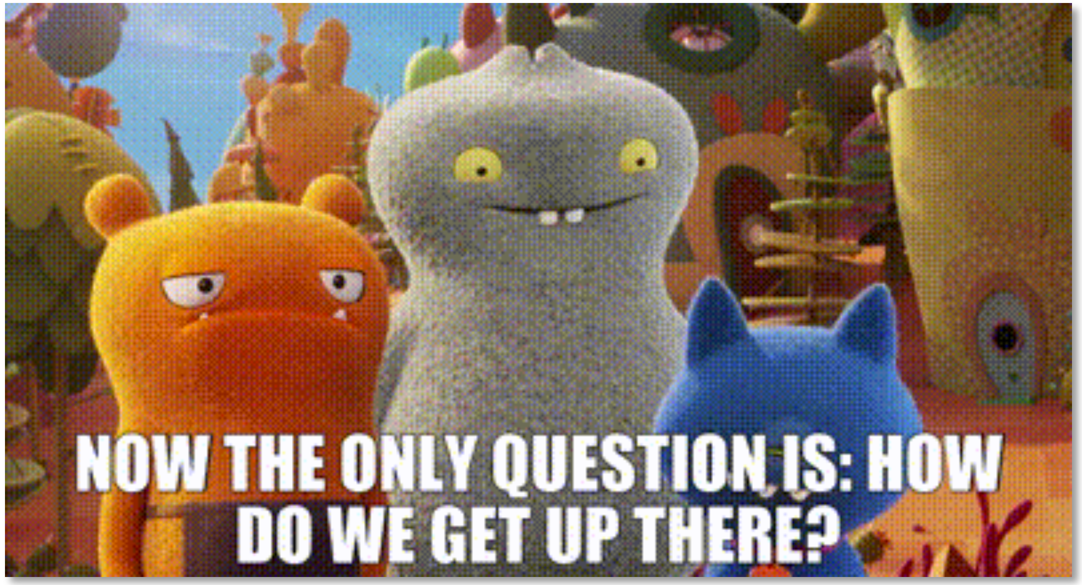
Timely & Actionable

Automated

Metrics and optimization

Constant Dialogue

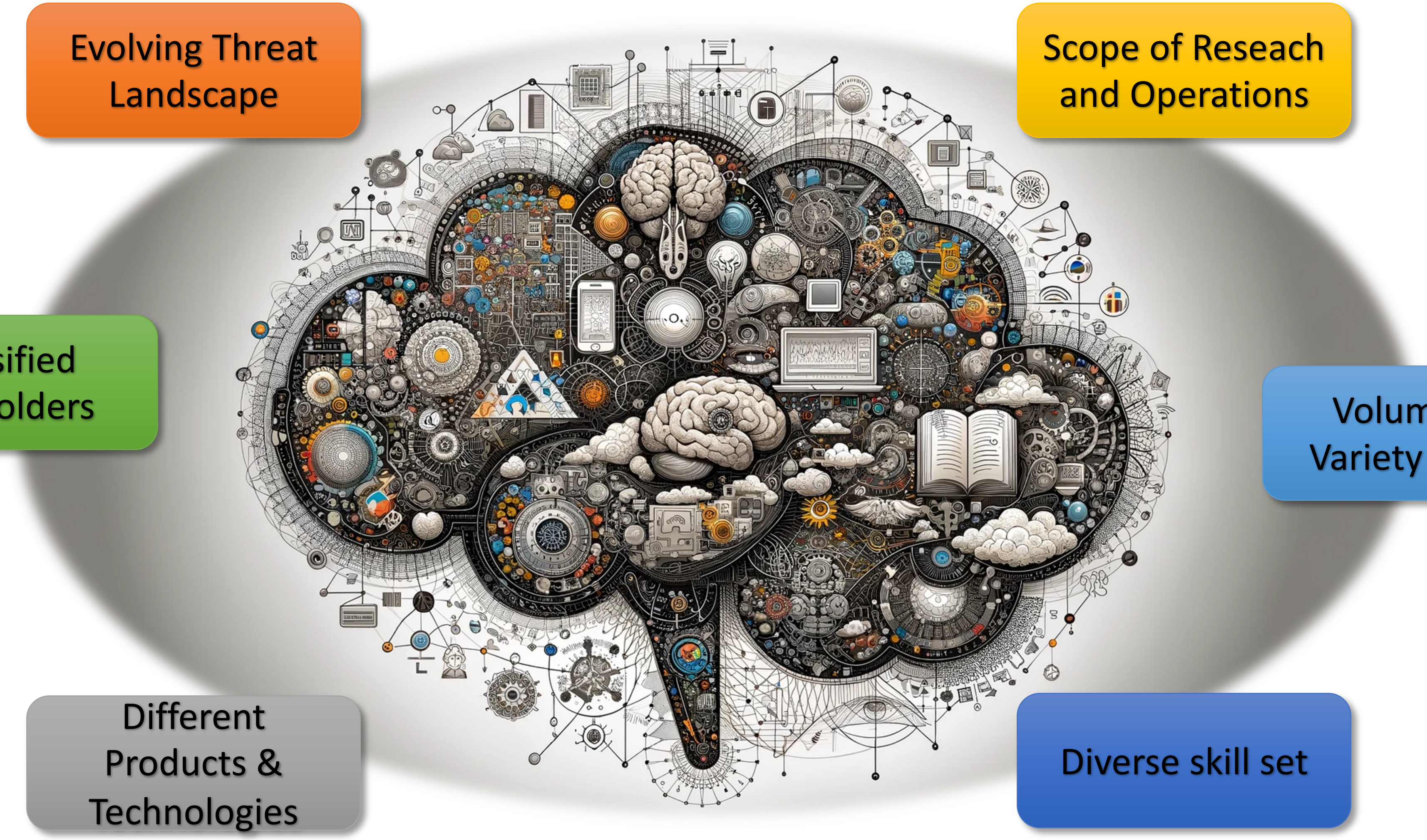
So how can we get there?



“But the intelligence is such a complex field…”

Evolving Threat Landscape

Scope of Reseach and Operations



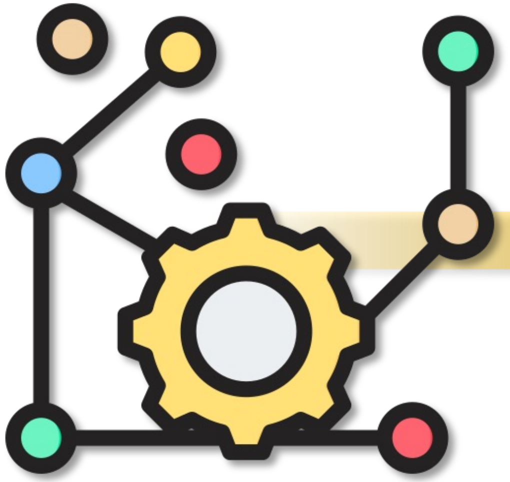
Diversified Stakeholders

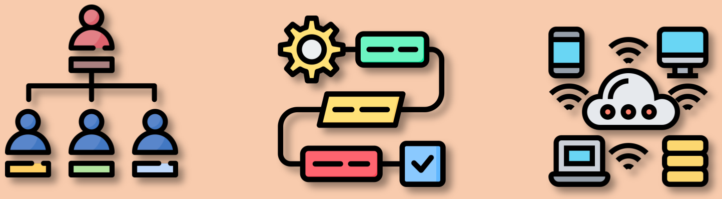
Volume and Variety of Data

Different Products & Technologies

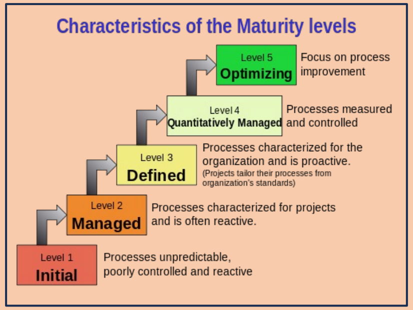
Diverse skill set

From complexity to simplicity





What defines CTI's role & impact?



Characteristics of the Maturity levels

Level 5 **Optimizing** – Focus on process improvement

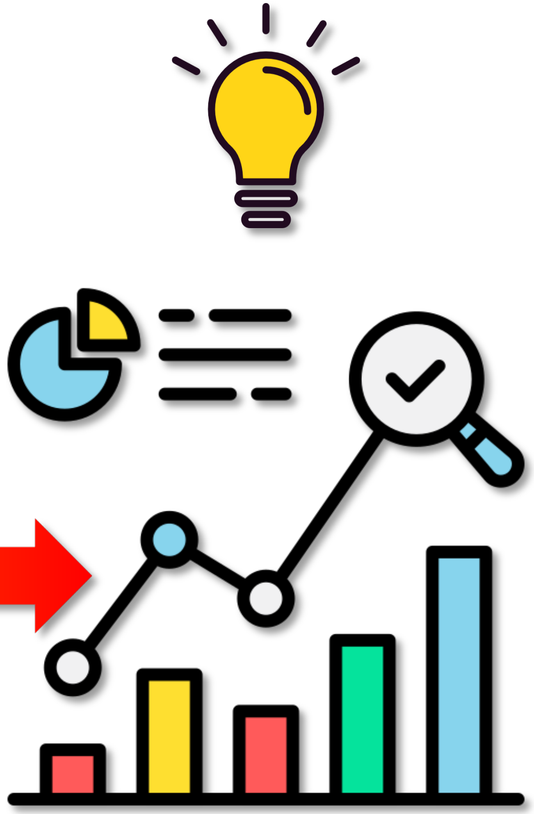
Level 4 **Quantitatively Managed** – Processes measured and controlled

Level 3 **Defined** – Processes characterized for the organization and is proactive. (Projects tailor their processes from organization's standards)

Level 2 **Managed** – Processes characterized for projects and is often reactive.

Level 1 **Initial** – Processes unpredictable, poorly controlled and reactive

How are other MMs structured?

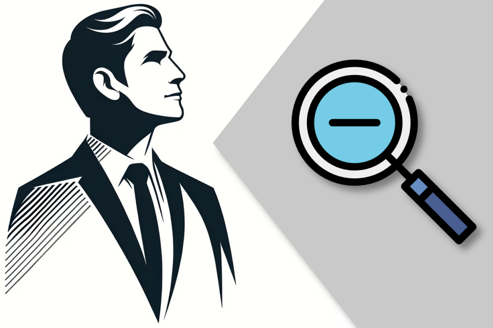


Trying not to „reinvent the wheel”

Soft.Dev. & CTI

1. Focus on security
2. Data-Driven Decision Making
3. Technology, Teamwork & Project Management
4. Continuous Learning & Adaptation

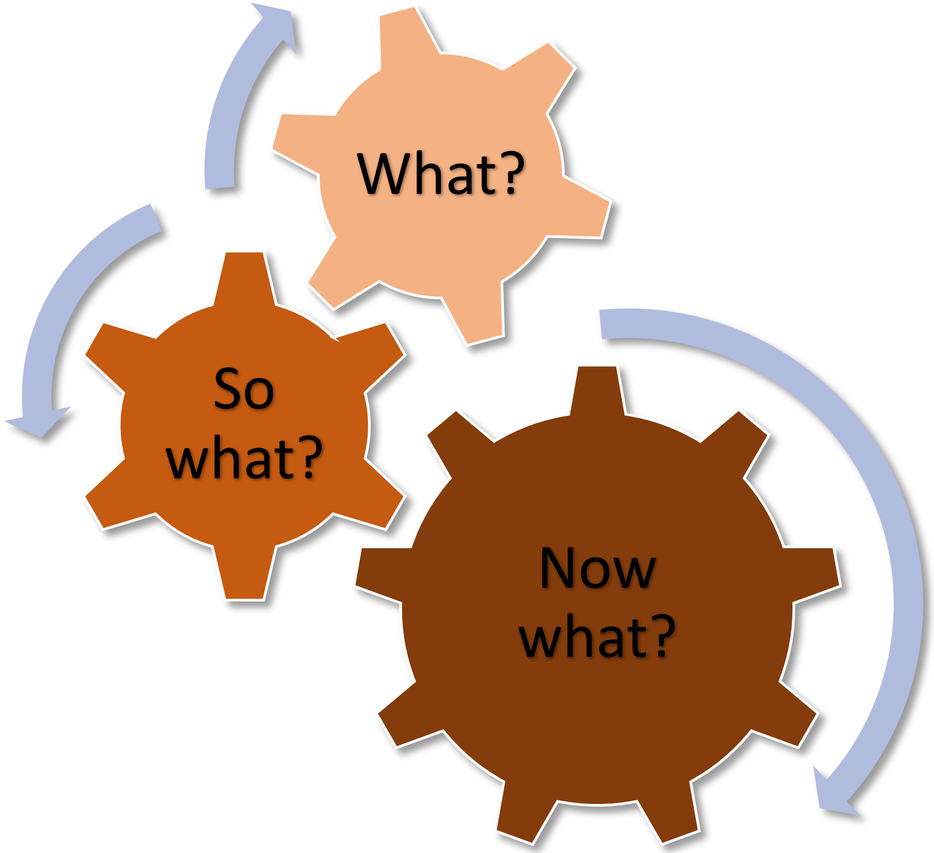
How to bring order into the design phase?



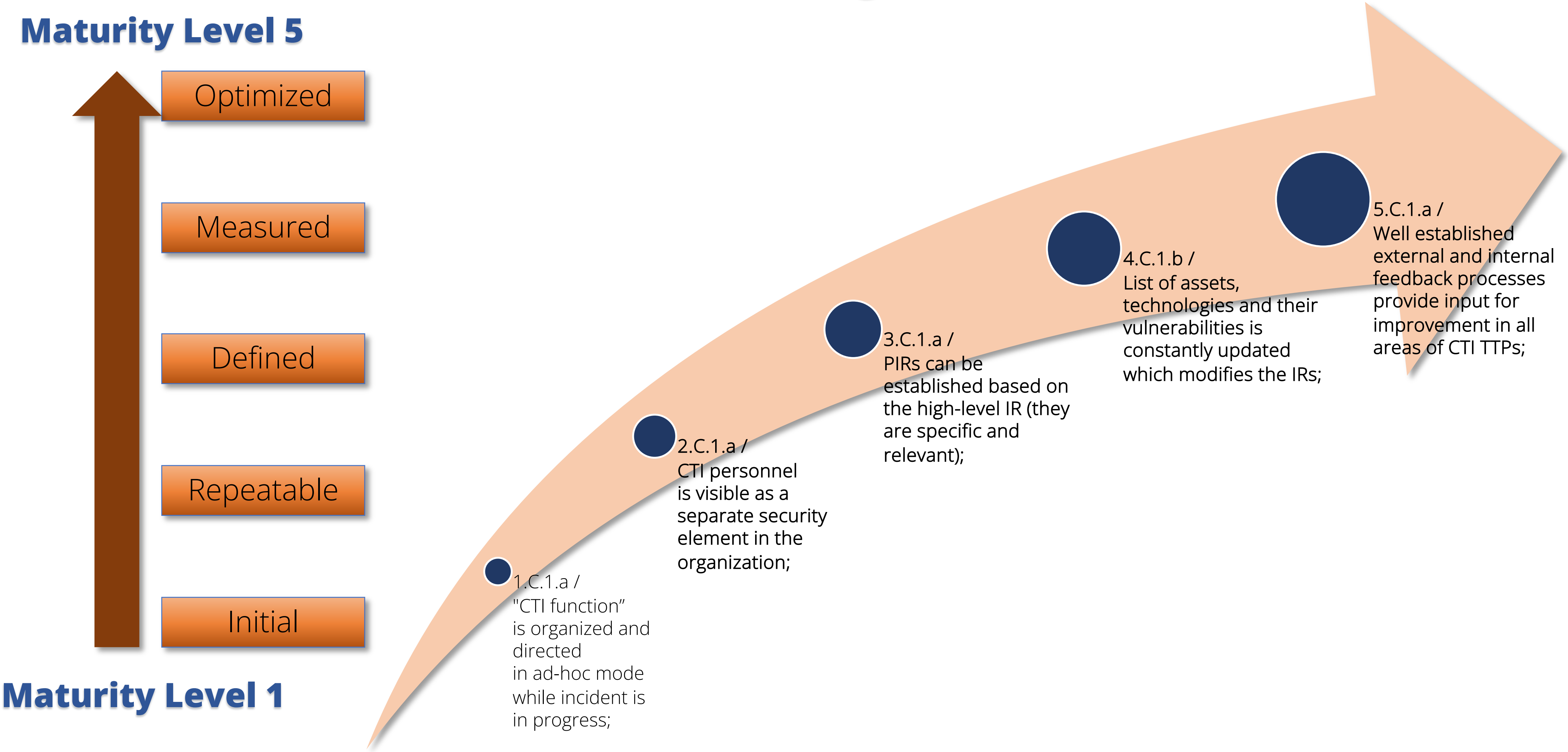
Initial	Repeatable	Defined	Measured	Optimized
No strategic direction, poor & ad-hoc coordination and communication	Simple coordination (personal contacts), repeating consulting, some shared decision making	Established comms and coordination channels, enable efficient direction and coordination	Collaborative workspace and culture in the organization, shared decision making, efficient feedback loop	Constant dialogue between stakeholders, based on the common understanding of concepts, processes and values
No automation, lots of manual work	Early stage of data aggregation, no central hub, well known tools used, technical controls added to the process	Data is semi – automatically aggregated in a central repository in unified manner	Most of the data collection and processing is done automatically from internal and external sources	Self-learning tools and technology are used in data collection, processing, initial triage and analysis
Chaotic, undefined, unpredictable, reactive	Simple, individual, not standardized processes, change with personnel rotation	Standardized, tested and documented processes in the organization	Processes are measured to gain insight into their efficiency, metrics enable temporal analysis	Processes are constantly evaluated and optimized

How to bring order into the design phase? – cont'd

- My goals
  - assess and improve
- Diagnostic Features
  - Identify clear indicators per level
  - Define process area activities, tailored for each maturity stag
- Prescriptive Pathways
  - Provide step-by-step growth guidance
  - Visualize activity evolution across maturity levels



„Now what?” - vertical thinking



1.C.1.a / "CTI function" is organized and directed in ad-hoc mode while incident is in progress;

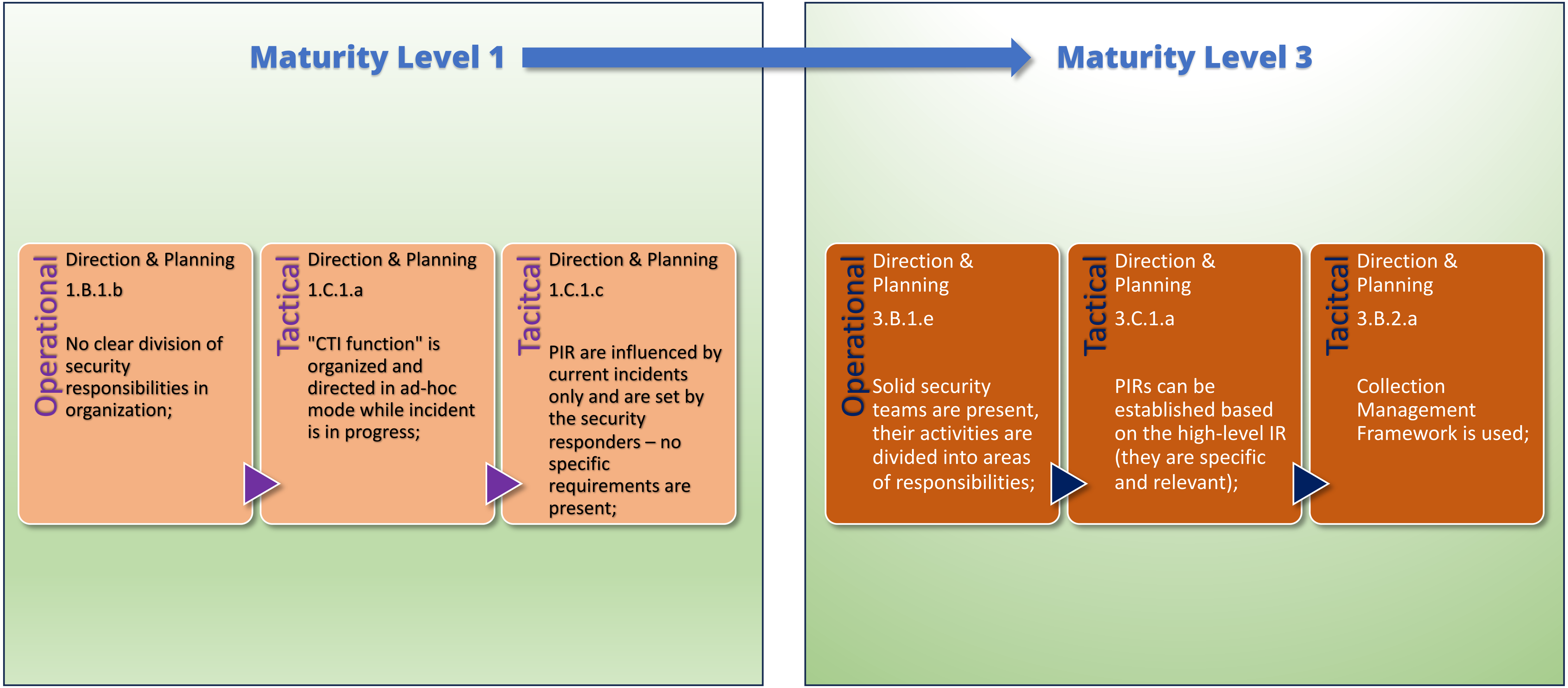
2.C.1.a / CTI personnel is visible as a separate security element in the organization;

3.C.1.a / PIRs can be established based on the high-level IR (they are specific and relevant);

4.C.1.b / List of assets, technologies and their vulnerabilities is constantly updated which modifies the IRs;

5.C.1.a / Well established external and internal feedback processes provide input for improvement in all areas of CTI TTPs;

“So what?” - horizontal thinking



Maturity Level 1

Maturity Level 3

Maturity Level 1

Operational

Direction & Planning

1.B.1.b

No clear division of security responsibilities in organization;

Tactical

Direction & Planning

1.C.1.a

"CTI function" is organized and directed in ad-hoc mode while incident is in progress;

Tacitcal

Direction & Planning

1.C.1.c

PIR are influenced by current incidents only and are set by the security responders – no specific requirements are present;

Maturity Level 3

Operational

Direction & Planning

3.B.1.e

Solid security teams are present, their activities are divided into areas of responsibilities;

Tactical

Direction & Planning

3.C.1.a

PIRs can be established based on the high-level IR (they are specific and relevant);

Tacitcal

Direction & Planning

3.B.2.a

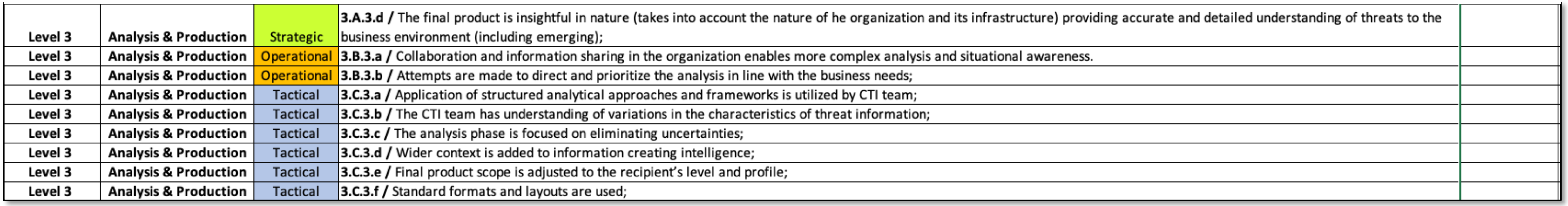
Collection Management Framework is used;

But what exactly should be „inside the controls"?

- ✓ What do controls mean?
- ✓ How detailed / broad should they be?

SMARF

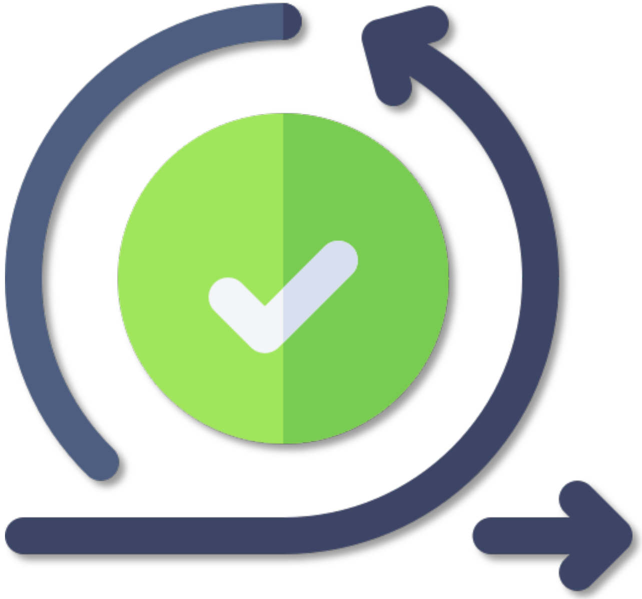
- Specific
- Measurability
- Achievability
- Relevance
- Flexibility



Maturity	Intel. Phase	Type	Control – content	Assessment
Level 3	**Analysis & Production**	Strategic	**3.A.3.d /** The final product is insightful in nature (takes into account the nature of he organization and its infrastructure) providing accurate and detailed understanding of threats to the business environment (including emerging);	
Level 3	**Analysis & Production**	Operational	**3.B.3.a /** Collaboration and information sharing in the organization enables more complex analysis and situational awareness.	
Level 3	**Analysis & Production**	Operational	**3.B.3.b /** Attempts are made to direct and prioritize the analysis in line with the business needs;	
Level 3	**Analysis & Production**	Tactical	**3.C.3.a /** Application of structured analytical approaches and frameworks is utilized by CTI team;	
Level 3	**Analysis & Production**	Tactical	**3.C.3.b /** The CTI team has understanding of variations in the characteristics of threat information;	
Level 3	**Analysis & Production**	Tactical	**3.C.3.c /** The analysis phase is focused on eliminating uncertainties;	
Level 3	**Analysis & Production**	Tactical	**3.C.3.d /** Wider context is added to information creating intelligence;	
Level 3	**Analysis & Production**	Tactical	**3.C.3.e /** Final product scope is adjusted to the recipient's level and profile;	
Level 3	**Analysis & Production**	Tactical	**3.C.3.f /** Standard formats and layouts are used;	

How to turn optimistic assumptions into deliverables?

High Level Methodology

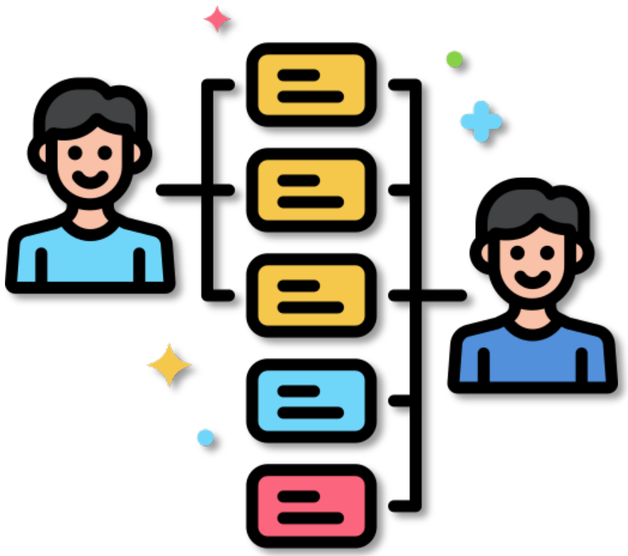


Evaluate

Start Small

Progress & Move On

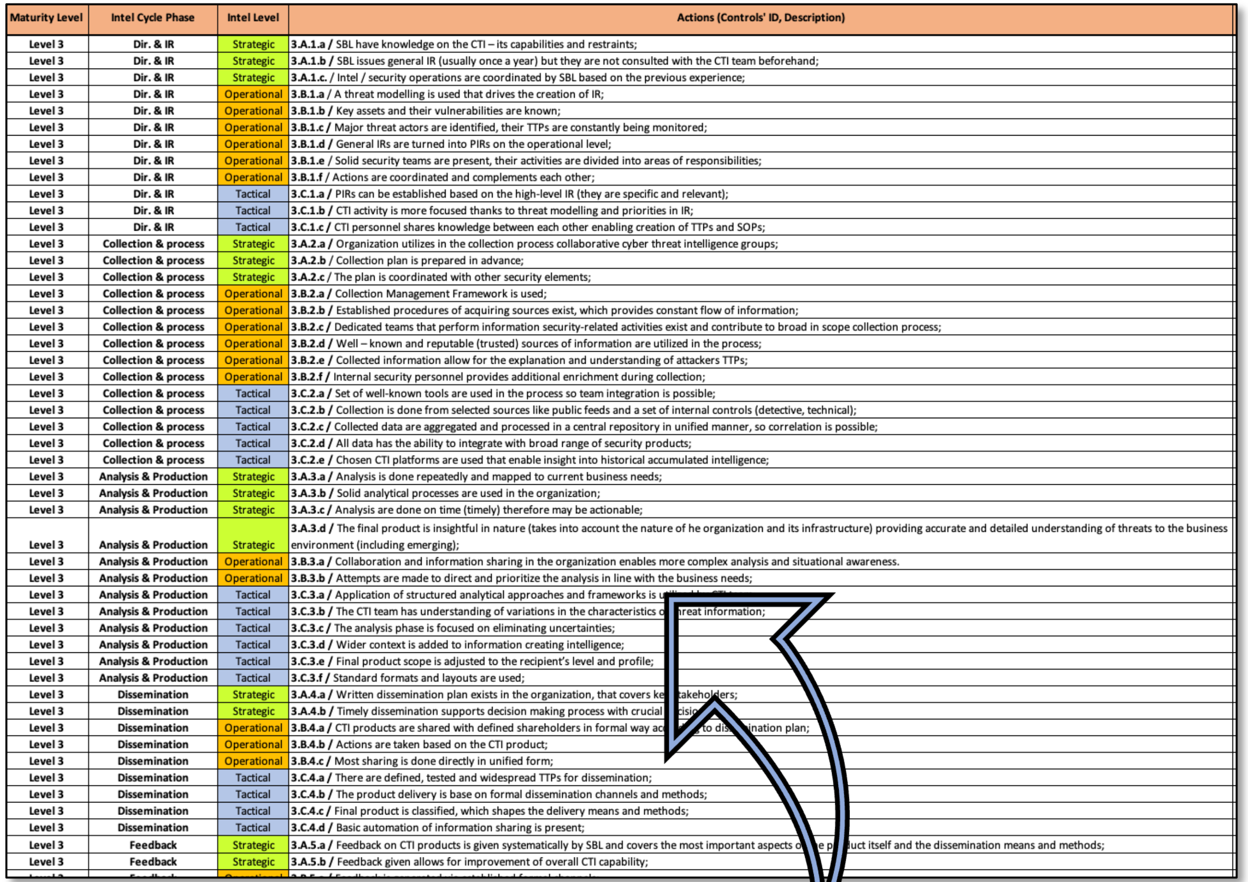
Low Level Approach



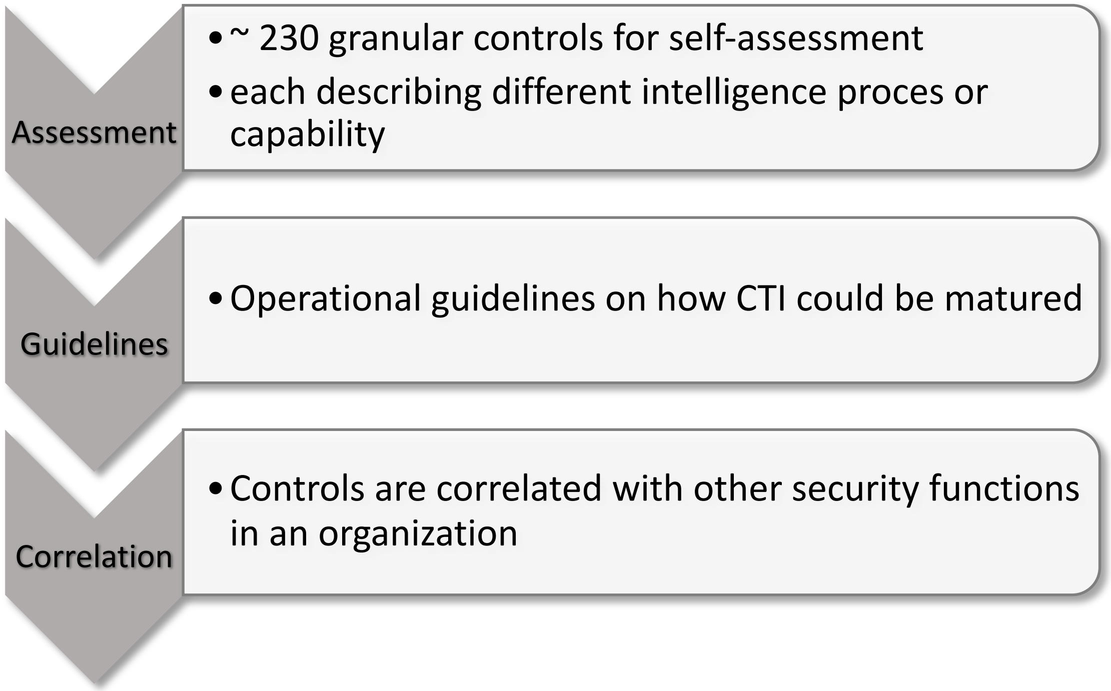
User Stories

Acceptance Criteria

How did it all end?



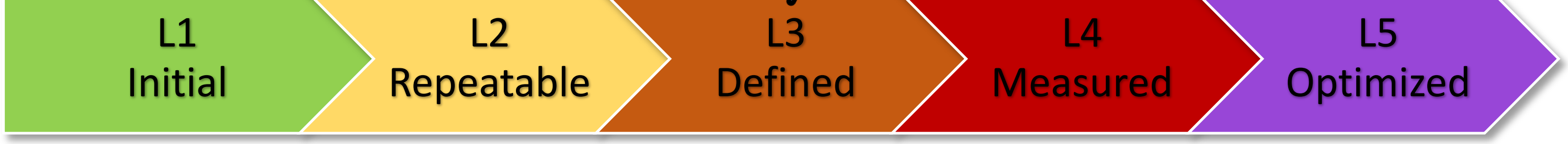
Maturity Level	Intel Cycle Phase	Intel Level	Actions (Controls' ID, Description)
Level 3	Dir. & IR	Strategic	**3.A.1.a /** SBL have knowledge on the CTI – its capabilities and restraints;
Level 3	Dir. & IR	Strategic	**3.A.1.b /** SBL issues general IR (usually once a year) but they are not consulted with the CTI team beforehand;
Level 3	Dir. & IR	Strategic	**3.A.1.c.** / Intel / security operations are coordinated by SBL based on the previous experience;
Level 3	Dir. & IR	Operational	**3.B.1.a** / A threat modelling is used that drives the creation of IR;
Level 3	Dir. & IR	Operational	**3.B.1.b /** Key assets and their vulnerabilities are known;
Level 3	Dir. & IR	Operational	**3.B.1.c /** Major threat actors are identified, their TTPs are constantly being monitored;
Level 3	Dir. & IR	Operational	**3.B.1.d /** General IRs are turned into PIRs on the operational level;
Level 3	Dir. & IR	Operational	**3.B.1.e** / Solid security teams are present, their activities are divided into areas of responsibilities;
Level 3	Dir. & IR	Operational	**3.B.1.f** / Actions are coordinated and complements each other;
Level 3	Dir. & IR	Tactical	**3.C.1.a /** PIRs can be established based on the high-level IR (they are specific and relevant);
Level 3	Dir. & IR	Tactical	**3.C.1.b /** CTI activity is more focused thanks to threat modelling and priorities in IR;
Level 3	Dir. & IR	Tactical	**3.C.1.c /** CTI personnel shares knowledge between each other enabling creation of TTPs and SOPs;
Level 3	Collection & process	Strategic	**3.A.2.a /** Organization utilizes in the collection process collaborative cyber threat intelligence groups;
Level 3	Collection & process	Strategic	**3.A.2.b** / Collection plan is prepared in advance;
Level 3	Collection & process	Strategic	**3.A.2.c** / The plan is coordinated with other security elements;
Level 3	Collection & process	Operational	**3.B.2.a /** Collection Management Framework is used;
Level 3	Collection & process	Operational	**3.B.2.b /** Established procedures of acquiring sources exist, which provides constant flow of information;
Level 3	Collection & process	Operational	**3.B.2.c /** Dedicated teams that perform information security-related activities exist and contribute to broad in scope collection process;
Level 3	Collection & process	Operational	**3.B.2.d /** Well – known and reputable (trusted) sources of information are utilized in the process;
Level 3	Collection & process	Operational	**3.B.2.e /** Collected information allow for the explanation and understanding of attackers TTPs;
Level 3	Collection & process	Operational	**3.B.2.f /** Internal security personnel provides additional enrichment during collection;
Level 3	Collection & process	Tactical	**3.C.2.a /** Set of well-known tools are used in the process so team integration is possible;
Level 3	Collection & process	Tactical	**3.C.2.b /** Collection is done from selected sources like public feeds and a set of internal controls (detective, technical);
Level 3	Collection & process	Tactical	**3.C.2.c /** Collected data are aggregated and processed in a central repository in unified manner, so correlation is possible;
Level 3	Collection & process	Tactical	**3.C.2.d /** All data has the ability to integrate with broad range of security products;
Level 3	Collection & process	Tactical	**3.C.2.e /** Chosen CTI platforms are used that enable insight into historical accumulated intelligence;
Level 3	Analysis & Production	Strategic	**3.A.3.a /** Analysis is done repeatedly and mapped to current business needs;
Level 3	Analysis & Production	Strategic	**3.A.3.b /** Solid analytical processes are used in the organization;
Level 3	Analysis & Production	Strategic	**3.A.3.c /** Analysis are done on time (timely) therefore may be actionable;
Level 3	Analysis & Production	Strategic	**3.A.3.d /** The final product is insightful in nature (takes into account the nature of he organization and its infrastructure) providing accurate and detailed understanding of threats to the business environment (including emerging);
Level 3	Analysis & Production	Operational	**3.B.3.a /** Collaboration and information sharing in the organization enables more complex analysis and situational awareness.
Level 3	Analysis & Production	Operational	**3.B.3.b /** Attempts are made to direct and prioritize the analysis in line with the business needs;
Level 3	Analysis & Production	Tactical	**3.C.3.a /** Application of structured analytical approaches and frameworks is u[illegible]
Level 3	Analysis & Production	Tactical	**3.C.3.b /** The CTI team has understanding of variations in the characteristics o[illegible]reat information;
Level 3	Analysis & Production	Tactical	**3.C.3.c /** The analysis phase is focused on eliminating uncertainties;
Level 3	Analysis & Production	Tactical	**3.C.3.d /** Wider context is added to information creating intelligence;
Level 3	Analysis & Production	Tactical	**3.C.3.e /** Final product scope is adjusted to the recipient's level and profile;
Level 3	Analysis & Production	Tactical	**3.C.3.f /** Standard formats and layouts are used;
Level 3	Dissemination	Strategic	**3.A.4.a /** Written dissemination plan exists in the organization, that covers ke[illegible]takeholders;
Level 3	Dissemination	Strategic	**3.A.4.b /** Timely dissemination supports decision making process with crucial [illegible]cisio[illegible]
Level 3	Dissemination	Operational	**3.B.4.a /** CTI products are shared with defined shareholders in formal way ac[illegible] to dis[illegible]ination plan;
Level 3	Dissemination	Operational	**3.B.4.b /** Actions are taken based on the CTI product;
Level 3	Dissemination	Operational	**3.B.4.c /** Most sharing is done directly in unified form;
Level 3	Dissemination	Tactical	**3.C.4.a /** There are defined, tested and widespread TTPs for dissemination;
Level 3	Dissemination	Tactical	**3.C.4.b /** The product delivery is base on formal dissemination channels and methods;
Level 3	Dissemination	Tactical	**3.C.4.c /** Final product is classified, which shapes the delivery means and methods;
Level 3	Dissemination	Tactical	**3.C.4.d /** Basic automation of information sharing is present;
Level 3	Feedback	Strategic	**3.A.5.a /** Feedback on CTI products is given systematically by SBL and covers the most important aspects o[illegible]e p[illegible]uct itself and the dissemination means and methods;
Level 3	Feedback	Strategic	**3.A.5.b /** Feedback given allows for improvement of overall CTI capability;
Level 3	Feedback	Operational	**3.B.5.a /** Feedback is generated via established formal channels;



- ~ 230 granular controls for self-assessment
- each describing different intelligence proces or capability

- Operational guidelines on how CTI could be matured

- Controls are correlated with other security functions in an organization

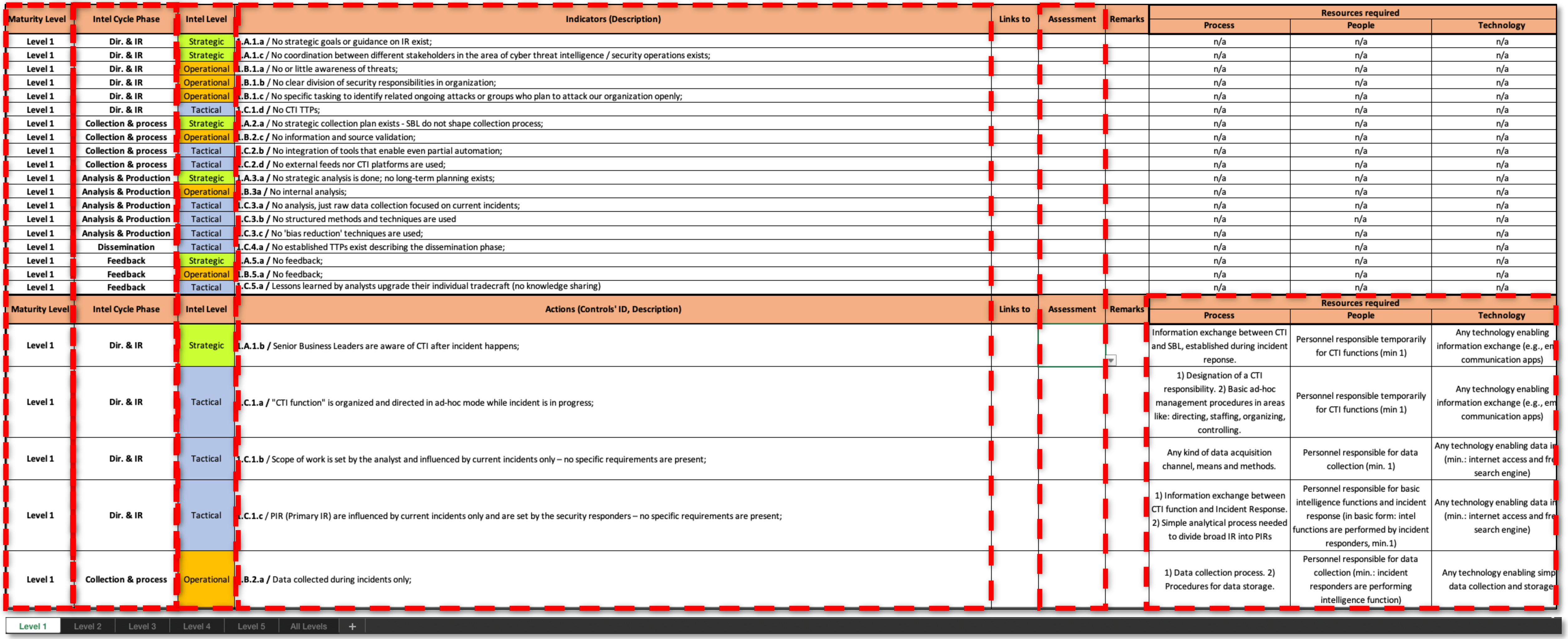


Make your own set!

How can I get it?

- ✓ https://github.com/Slavkey/CTI_Maturity_Model
- ✓ CMM_maturity_model.xlsx
- ✓ What is it?
- ✓ Who is it for?
- ✓ What's the purpose?

What’s inside ?



Maturity Level	Intel Cycle Phase	Intel Level	Indicators (Description)	Links to	Assessment	Remarks	Resources required		
							Process	People	Technology
Level 1	Dir. & IR	Strategic	**1.A.1.a** / No strategic goals or guidance on IR exist;				n/a	n/a	n/a
Level 1	Dir. & IR	Strategic	**1.A.1.c** / No coordination between different stakeholders in the area of cyber threat intelligence / security operations exists;				n/a	n/a	n/a
Level 1	Dir. & IR	Operational	**1.B.1.a** / No or little awareness of threats;				n/a	n/a	n/a
Level 1	Dir. & IR	Operational	**1.B.1.b** / No clear division of security responsibilities in organization;				n/a	n/a	n/a
Level 1	Dir. & IR	Operational	**1.B.1.c** / No specific tasking to identify related ongoing attacks or groups who plan to attack our organization openly;				n/a	n/a	n/a
Level 1	Dir. & IR	Tactical	**1.C.1.d /** No CTI TTPs;				n/a	n/a	n/a
Level 1	Collection & process	Strategic	**1.A.2.a** / No strategic collection plan exists - SBL do not shape collection process;				n/a	n/a	n/a
Level 1	Collection & process	Operational	**1.B.2.c /** No information and source validation;				n/a	n/a	n/a
Level 1	Collection & process	Tactical	**1.C.2.b /** No integration of tools that enable even partial automation;				n/a	n/a	n/a
Level 1	Collection & process	Tactical	**1.C.2.d /** No external feeds nor CTI platforms are used;				n/a	n/a	n/a
Level 1	Analysis & Production	Strategic	**1.A.3.a /** No strategic analysis is done; no long-term planning exists;				n/a	n/a	n/a
Level 1	Analysis & Production	Operational	**1.B.3a /** No internal analysis;				n/a	n/a	n/a
Level 1	Analysis & Production	Tactical	**1.C.3.a /** No analysis, just raw data collection focused on current incidents;				n/a	n/a	n/a
Level 1	Analysis & Production	Tactical	**1.C.3.b /** No structured methods and techniques are used				n/a	n/a	n/a
Level 1	Analysis & Production	Tactical	**1.C.3.c** / No 'bias reduction' techniques are used;				n/a	n/a	n/a
Level 1	Dissemination	Tactical	**1.C.4.a /** No established TTPs exist describing the dissemination phase;				n/a	n/a	n/a
Level 1	Feedback	Strategic	**1.A.5.a /** No feedback;				n/a	n/a	n/a
Level 1	Feedback	Operational	**1.B.5.a /** No feedback;				n/a	n/a	n/a
Level 1	Feedback	Tactical	**1.C.5.a /** Lessons learned by analysts upgrade their individual tradecraft (no knowledge sharing)				n/a	n/a	n/a

Maturity Level	Intel Cycle Phase	Intel Level	Actions (Controls' ID, Description)	Links to	Assessment	Remarks	Resources required		
							Process	People	Technology
Level 1	Dir. & IR	Strategic	**1.A.1.b /** Senior Business Leaders are aware of CTI after incident happens;				Information exchange between CTI and SBL, established during incident reponse.	Personnel responsible temporarily for CTI functions (min 1)	Any technology enabling information exchange (e.g., em communication apps)
Level 1	Dir. & IR	Tactical	**1.C.1.a** / "CTI function" is organized and directed in ad-hoc mode while incident is in progress;				1) Designation of a CTI responsibility. 2) Basic ad-hoc management procedures in areas like: directing, staffing, organizing, controlling.	Personnel responsible temporarily for CTI functions (min 1)	Any technology enabling information exchange (e.g., em communication apps)
Level 1	Dir. & IR	Tactical	**1.C.1.b** / Scope of work is set by the analyst and influenced by current incidents only – no specific requirements are present;				Any kind of data acquisition channel, means and methods.	Personnel responsible for data collection (min. 1)	Any technology enabling data i (min.: internet access and fr search engine)
Level 1	Dir. & IR	Tactical	**1.C.1.c** / PIR (Primary IR) are influenced by current incidents only and are set by the security responders – no specific requirements are present;				1) Information exchange between CTI function and Incident Response. 2) Simple analytical process needed to divide broad IR into PIRs	Personnel responsible for basic intelligence functions and incident response (in basic form: intel functions are performed by incident responders, min.1)	Any technology enabling data i (min.: internet access and fr search engine)
Level 1	Collection & process	Operational	**1.B.2.a /** Data collected during incidents only;				1) Data collection process. 2) Procedures for data storage.	Personnel responsible for data collection (min.: incident responders are performing intelligence function)	Any technology enabling simp data collection and storage

How should I start ?

Review the model

- ✓ Understand the big picture
- ✓ Delve into controls

Self – assess

- ✓ Start with 1 and advance till you can

Prioritize

- ✓ Understand actual business needs
- ✓ Set goals and priorities
- ✓ See how controls depend on each – other

How should I progress ?

PLAN
3
LEVEL

Plan

- ✓ People, processes, technology
- ✓ Budget
- ✓ Deadlines

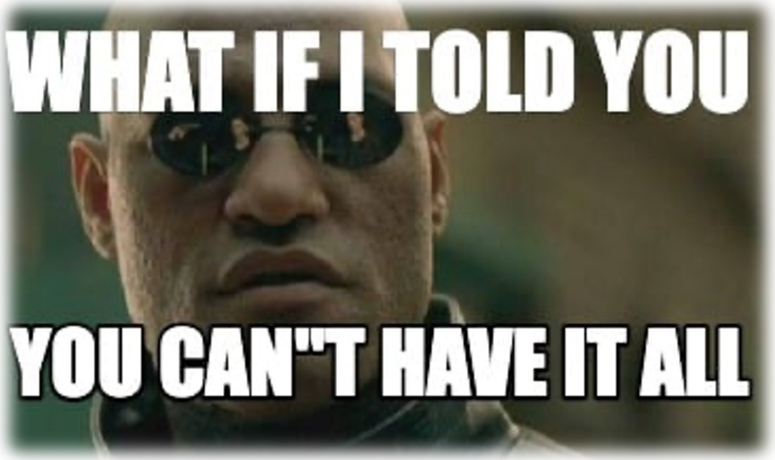
Deliver

- ✓ Set goals and priorities
- ✓ See how controls depend on each – other

Re-assess

- ✓ Conduct reassessment
- ✓ … and continue

When / how does it end?



Initial

Repeatable

Defined

Measured

Optimized

2024
FIRST
Cyber Threat
Intelligence
Conference

Berlin, Germany
April 15-17, 2024

Thank you!

Questions?

if later: https://www.linkedin.com/in/slawek-kiraga

FIRST
Improving Security Together