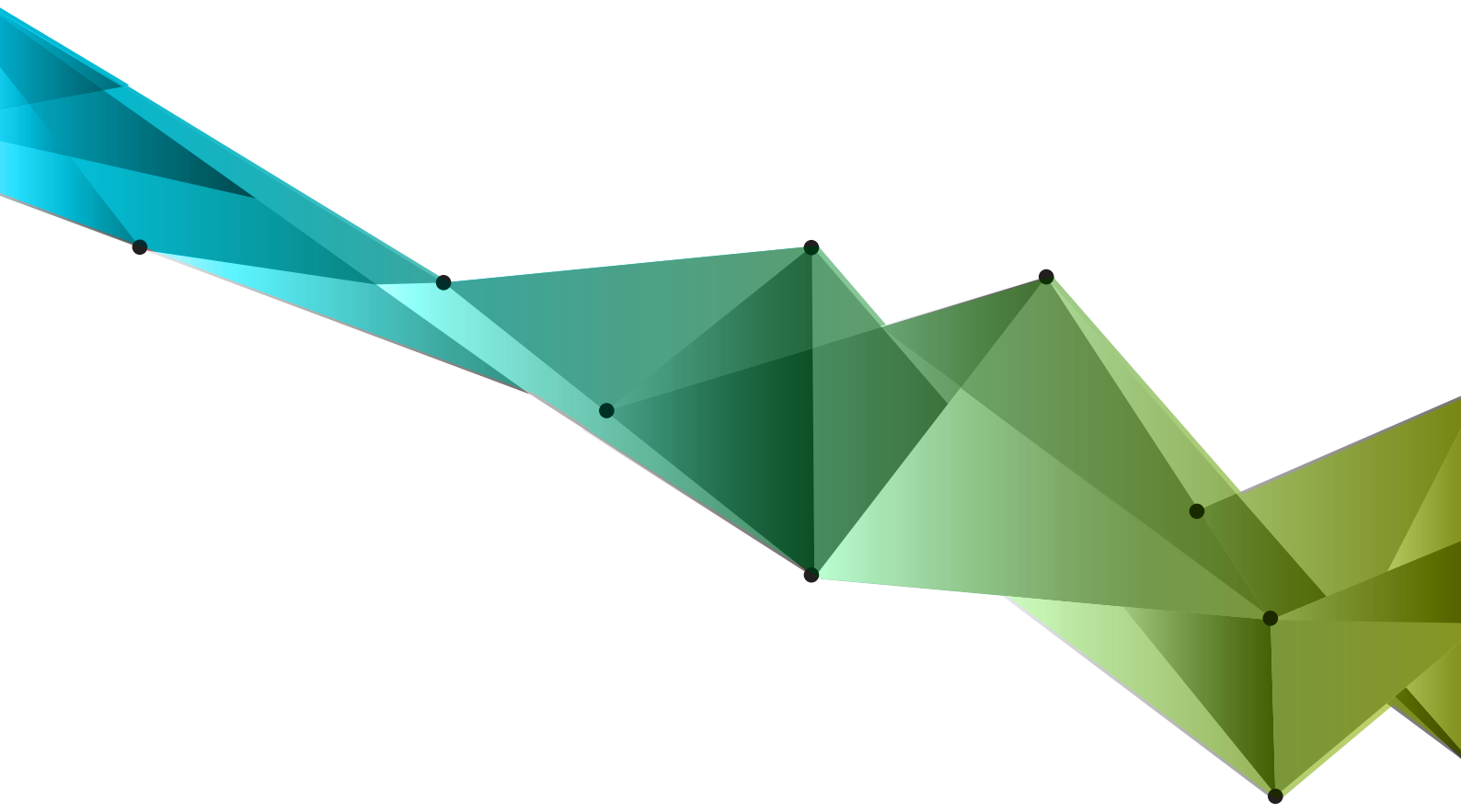
Mark Luchs - Christian Doerr

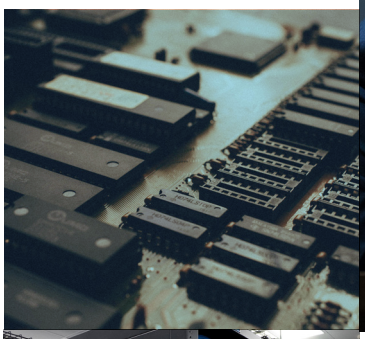
Measuring Your Cyber Threat Intelligence Maturity

A 5-Minute Introduction

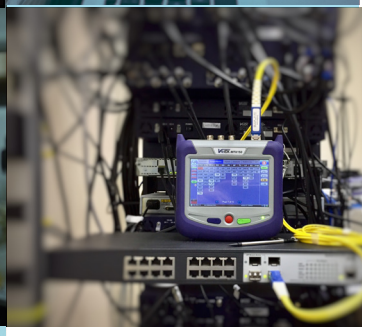


HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

TU Delft


imgIX





Why Measure Cyber Threat Intelligence?

Our CTI maturity model gives organizations insights into their current cyber threat intelligence capabilities, and points out opportunities to produce and make better use of CTI.

To determine your CTI maturity level and receive your personalized report, visit

https://www.cyber-threat-intelligence.com/maturity

In order to defend yourself, you have to know what you are up against. Who are actors that might attack your organization? How will they work? What are they trying to do? And if there is a potential attack vector, what will be the impact on your business? Only if you have insights into your cyber risk profile, it is possible to plan an effective defense to mitigate these threats efficiently.

This information is provided by the emerging field of cyber threat intelligence, an essential input to addressing and treating the risks your organization faces.

Why measure your maturity?

While a cyber threat intelligence program can offer important benefits to the cyber security of your organization, building such a new function from scratch is a challenging task. Also, even if a CTI program exists, it provides only full value if the necessary preparations are done, the right activities are conducted, and information integrated in the right places.

To help organizations assess their current CTI capabilities, we have developed the cyber threat intelligence maturity model (CTIM). By participating in a survey of 250 questions, CTIM provides an analysis of your organization's current state, identifies strong and weak points in its current CTI-related activities, and makes a set of suggestions on which activities and investments could be done as next steps to produce and make better use of CTI. In this respect, CTIM complements other maturity models. While these for example assess the general state of cyber security, CTIM provides specific insights into how to build and improve your cyber threat intelligence program.

Who is this model for?

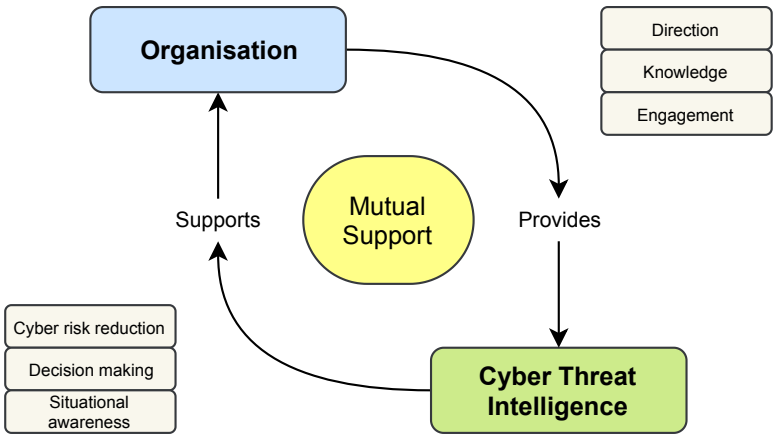
Anyone working in the field of cyber security and cyber threat intelligence. Specifically, the maturity rating and recommendations will be of use to top-level management, L3 analysts, SOC leads, security officers, etc.

A Model for Cyber Threat Intelligence Maturity

The purpose of cyber threat intelligence is to reduce cyber risk. This support is provided through the integration of specific threat intelligence products. These help stakeholders throughout the organization with their decision making, and increase an organization's situational awareness.

Organizational Support of Cyber Threat Intelligence Activities

For CTI to be effective, it needs to be embedded and tightly integrated throughout the organization. On the one hand, cyber threat intelligence requires direction, knowledge and engagement from the organization. Without input from stakeholders on their assets and concrete information requirements, it is not possible to collect cyber threat intelligence that is relevant and fits the needs of the organization. For example, if the people who create CTI do not know what kind of systems, software and infrastructure is running, they cannot be on watch for potential threats targeting these resources.



On the other hand, threat intelligence is only effective if it is absorbed by the organization and is integrated in the right places. For instance, when the group has received intelligence how a threat actor has been able to compromise other companies in your sector through some new type of spear-phishing attack, this information has to be put into practice to be useful, such as being loaded into intrusion detection systems and disseminated as an alert message or awareness training to your staff.

Organizations that have a mature cyber threat intelligence capability, have established this mutual support and put business processes in place that generate high quality threat intelligence, integrate it and support the CTI activities at essential points across the organization.

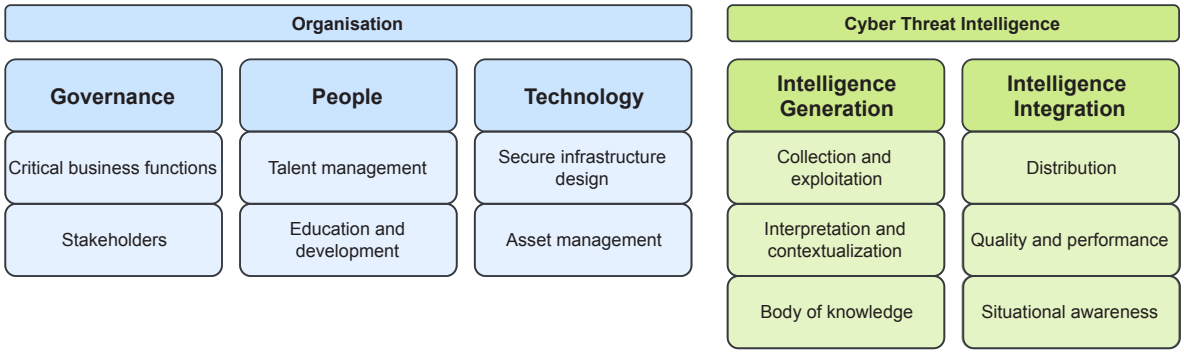
The CTI Maturity Model (CTIM)

Through observation of successful CTI programs, expert interviews and field research, we identified 5 domains and 12 different themes we call focus areas which are important to a successful CTI program.

Governance provides the organisational leadership for the consumption and production of CTI. The business objective, critical assets, and stakeholders interact with the team responsible for CTI, and make requests for intelligence products that help them in their decision making. In the CTIM model, we thus assess how management and stakeholders provide direction, and utilize the CTI results.

Measuring Your Cyber Threat Intelligence Maturity

CTI can provide the most benefit if it is integrated throughout the organization. Your CTI team needs direction and stakeholder interaction, but the organization needs to be prepared to absorb the CTI results at the right places.



People are at the heart of every organisation. For a CTI program to be successful, an organization needs to bring together people with many different types of expertise and specializations. The model looks in terms of People at the resources made available to CTI, the internal development of skills required for CTI, and how functions essential for CTI are located and defined throughout the organization.

T**echnology** supports and realizes an organization's critical business functions. These assets, ranging from computers to network infrastructure, are also the target or means of attack for cyber threats. For CTI to be successful, it is vital that the organization understands its security controls, provides means for threat intelligence to be used to improve its defenses, and has insight into its technical assets. In the survey, the CTIM model measures this integration for succesfull utilization of CTI.

Generation and Integration of CTI

Intelligence is a process, a product and a business function. Within the two domains Intelligence Generation and Intelligence Integration we assess the activities that are necessary to produce threat intelligence that is of high quality, actionable and timely, and investigate whether the created intelligence products fully meet the requirements of the stakeholders.

For successful **Intelligence Generation**, the organization needs to identify and collect the right type of data best suited to answer its intelligence needs. Data also needs to be validated and contextualized to become useful for decision makers, and repeated investigations should create a body of knowledge in terms of tradecraft and intelligence results to not look at individual pieces of data, but put information into context and arrive at a long-term global view of the threat landscape it faces.

The successful absorption of threat intelligence throughout the organization is first an issue of creating interest by stakeholders, but is also requires technical, legal, and procedural groundwork. **Intelligence Integration** assesses the maturity of the organization from this perspective, and investigates whether feedback loops exist to continuously improve the CTI program and meet its objectives.

Assess and Improve **Your CTI Maturity**

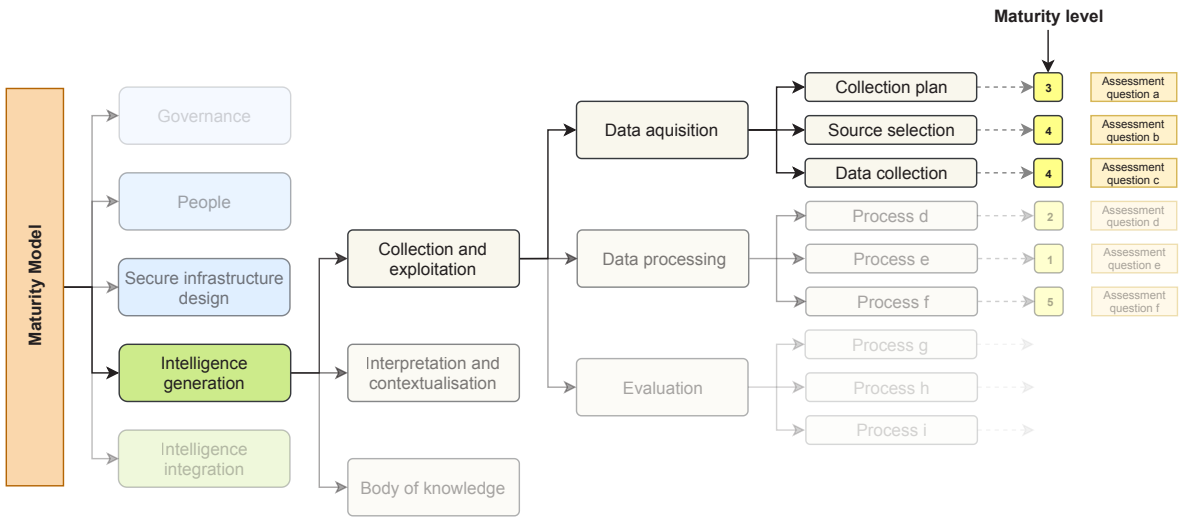
From Domains to Business Processes

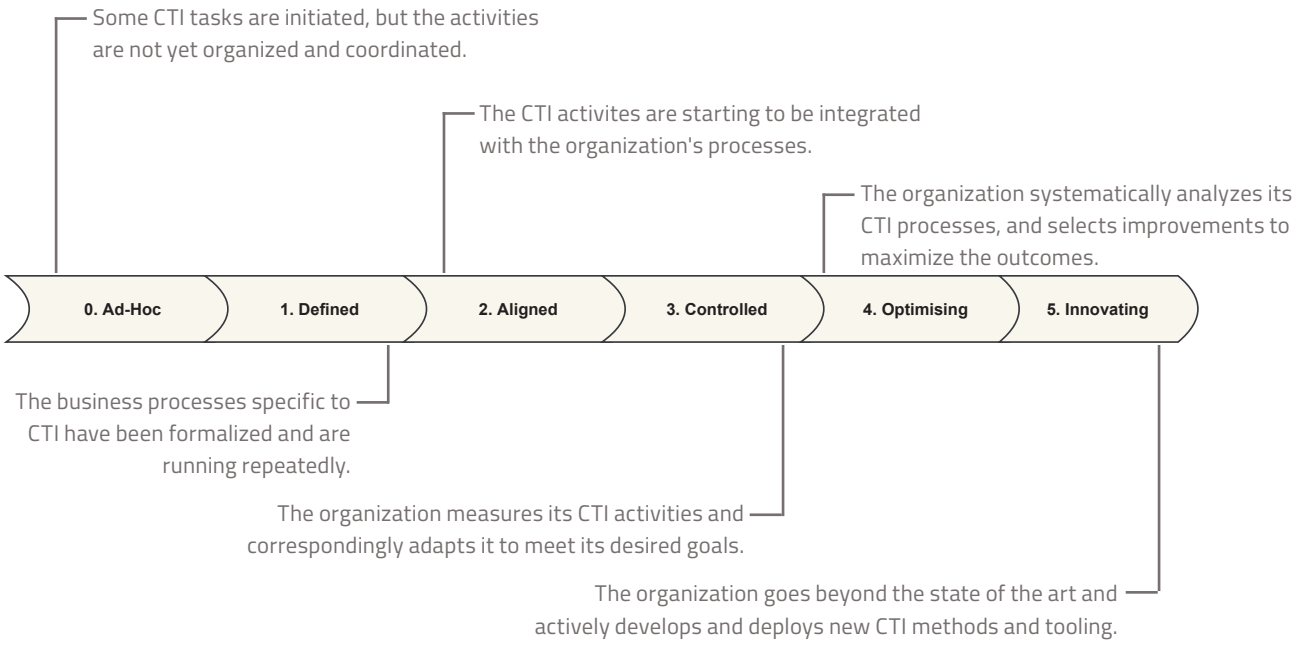
Based on the domains of CTI generation and integration as well as the organizational support functions Governance, People and Technology, we analyzed and decomposed each of the focus areas into 29 process groups and 83 concrete business processes and activities that organizations would run to realize the development and support of their cyber threat intelligence program.

Not all of these business processes will be of equal importance, for example a large multinational will require a different CTI generation and support structure than a small- or medium enterprise, also an organization just starting out with CTI will pursue different activities than an organization with a mature program.

We hence rank each business process and rate it with a maturity level ranging from 0 to 5, in other words determine whether this is an essential activity for the successful start of a CTI program, whether it will provide benefit only later on once the business processes around the generation, integration and support of threat intelligence have sufficiently matured, or it is an activity only relevant for highly advanced use cases.

In the CTIM survey, we ask you a set of 250 questions that help us assess which activities you are currently pursuing, to which extent you are implementing these processes, and how these processes are connected throughout the organization. From this, we compute your maturity at the level of focus areas and domains as shown below and thus provide you with very detailed insight on your current level of cyber threat intelligence in your organization, as well as provide recommendations on how to continue the development of your program.

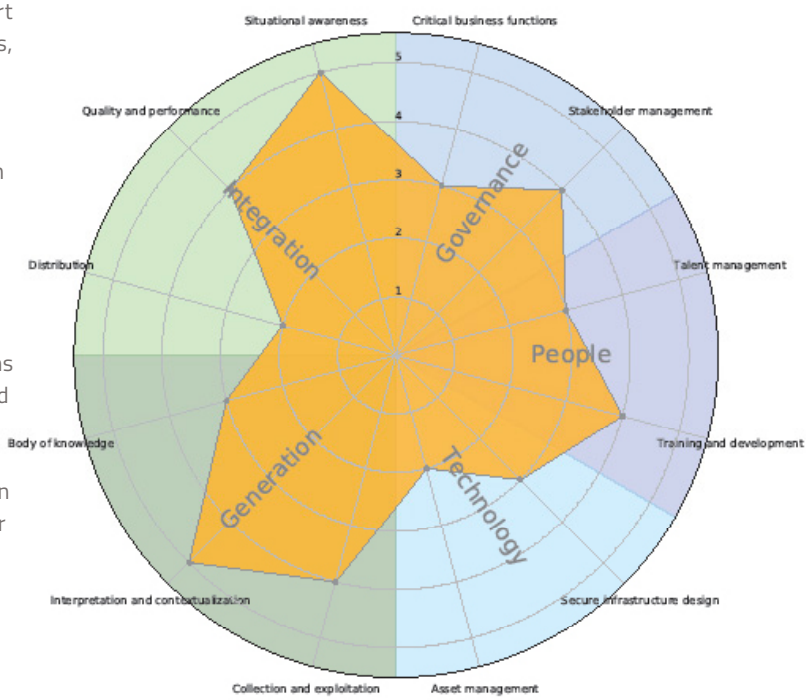




Your Current CTI Maturity and Opportunities for Improvement

After the survey, you will receive a report characterizing your current CTI activities, and the maturity of the CTI program in your organization. This analysis includes a classification of the maturity of your entire CTI program, as well as an investigation by domain and focus area.

In addition to this, your report also contains a list of recommendations on how to bring your current CTI activities to the next level and increase the returns you can gain from your program. Ranked by importance and impact to advance your organization as a whole, we determine focus areas to concentrate on to achieve the next level of maturity. For each of the focus areas, we recommend measures and activities that you could deploy or focus your attention on as a next logical step, and supply specific examples. This provides you with input to your personal roadmap to develop and further improve your CTI program.



Determine Your Cyber Threat Intelligence Maturity Level

To determine your CTI maturity level and receive your personalized report, visit

https://www.cyber-threat-intelligence.com/maturity

The data collected will only be used for the generation of your analysis report and collated in an anonymized form to make aggregated comparisons such as sectors or regions.

Reach the Cyber Threat Intelligence Lab at

Hasso Plattner Institut
Chair of Cybersecurity and Enterprise Security
Prof. Dr. Christian Doerr
Rudolf Breitscheid Strasse 187-189
14482 Potsdam, Germany

Delft University of Technology
Cyber Security Group
Dr. Christian Doerr
Van Mourikbroekmanweg 6
2628XE Delft, Netherlands