
ThreatConnect.
ThreatConnect's
Threat Intelligence
Maturity Model (TIMM)
Learn how to plan, assess, and mature a
cyber threat intelligence program

Introduction

A threat intelligence program is critical for cybersecurity operations, yet they have not been adopted widely, and where adopted, maturity varies by organization. Some organizations have made significant investment in people, processes, and tools over several years to achieve a high maturity level. Most organizations are still climbing the maturity curve. Increasing the maturity of the threat intel program is not dependent upon just money (e.g., for more people and tools). It requires strategic investment in analyst time, the right solutions, and support from the rest of the cybersecurity team and leadership.

Whether you are a threat intel team of one, or 10, it's achievable to mature the function to deliver more value to the organization with the right planning and investments.

What exactly is cyber threat intelligence (CTI)?

> "Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes." [1]

1 NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing

The Challenge

Many security operations teams don't have the necessary awareness and insights about the threats their organizations face, and they are not collaborating effectively (if at all) with the threat intel team. Security operations teams are stuck in a reactive or compliance-driven approach to cybersecurity with no clear vision or blueprint for reaching a better state.

In the rush to implement threat intelligence capabilities, organizations are purchasing standalone services and tools that work in silos, making it difficult to achieve a threat intel program that is collaborative, efficient, effective, and delivering value to stakeholders and the organization.

> Going beyond simple data aggregation and analysis is a prerequisite for any useful threat intelligence program.

Yet, it's not enough to buy some threat intel services and tools. In order to fully harness the power of threat intel, your organization must make the case for an intelligence-powered approach with the right people to staff the program and build processes to fully utilize the investment in intel services and tools. In order to evolve a defensive posture capable of resisting attacks from even the most persistent and aggressive threat actors, you must source the right threat data, sift through the noise, discover and implement the right process and methodologies, implement automation, and improve information sharing internally between teams and externally with industry peers, supply chain partners, and others.

Of course, not all organizations have the resources and organizational structures needed to implement a comprehensive threat intelligence program. And that's fine. Threat intelligence is an iterative process with defined maturity levels and milestones.

A Solution

ThreatConnect specializes in delivering high-value threat intelligence outcomes, so we developed the **Threat Intelligence Maturity Model (TIMM)** to help organizations address the challenges and realize the benefits of their CTI investments. Whether your organization is just getting started with CTI or seeking to expand an existing program, the TIMM provides a systematic guide to help your organization plan the path to starting and maturing a threat intelligence program; and how to better apply threat intelligence to identify threats faster, drive smarter security processes, and take decisive action to keep your business safe and resilient to threats.

The Threat Intelligence Maturity Model

To find out more about where your organization is on the Threat Intelligence Maturity Model, review each stage and learn what defines each one across people, processes, technology, and organizational dynamics in order to operationalize your organizations' threat intelligence. The model provides direction and offers opportunities to grow at each stage, as well as challenges to anticipate as you move to the next level.

THREAT INTELLIGENCE **MATURITY LEVELS**

MATURITY LEVEL 1
INITIAL

Getting Started

MATURITY LEVEL 2
MANAGED

Warming Up to Threat Intelligence

- Aggregate threat data for alerting and blocking
- Consume Threat Intelligence

MATURITY LEVEL 3
DEFINED

Expanding Threat Intelligence Capabilities

- Produce some operational TI
- Consume Threat Data and TI
- Automate some Threat Intelligence analyst tasks

MATURITY LEVEL 4
QUANTITATIVELY MANAGED

An Established Threat Intelligence Operations Program in Place

- Some TI Processes and Workflows
- Create tactical and strategic TI
- Automate some Threat Intelligence analyst tasks

MATURITY LEVEL 5
OPTIMIZING

A Well-Defined Threat Intelligence Operations Program

- Mature CTI skills and processes
- Producing a range of intel outputs (operational, tactical and strategic)
- Automate as much as possible
- Advanced analytics and orchestration capabilities
- Proactively hunt threats

MATURITY LEVEL 1 | INITIAL

Getting Started

Threat intelligence programs begin life as threat intel data collection programs. Many organizations start out with ad-hoc processes and seek external feeds and news sources, like open source intelligence (OSINT). With no existing centralized threat repository, this can create a big data problem, e.g., volume, velocity, variety, and veracity of data. Data at this stage is "one size fits none," meaning that it is raw and unformatted, has no context around it, and makes it very difficult to deduce how to thwart cyber threats.

Where do you put this data? Most organizations keep this information in massive spreadsheets or never ending email chains, while some feed it directly into their SIEM or firewall without any refinement, usually leading to a lot of false positives and the feeds eventually being turned off by owners of the security tools.

MATURITY LEVEL 1 | INITIAL

Recommendations

A good starting place involves aggregating internal data and external feeds from multiple sources and cross-referencing it to discover patterns and weed out false positives. Threat data, like indicators of compromise (IOCs), can then be sent to your endpoint, network, and cloud threat detection and prevention tools.

As you start aggregating your data, it is a good time to start thinking about storing the data in a more reliable place. Copying and pasting threat data into a spreadsheet not only takes an enormous amount of time, but also makes it hard to find the information quickly in the future. And let's be honest, no one reads massive email chains. You need a repository that is the system of record: a place to put all of your threat data that is easily accessible and searchable. This will make future maturity levels much easier to achieve.

You may be tempted to build your own threat intel repository and tool, but there are many arguments against that – cost, time, effort, and sustainability. Rather than use your limited, highly-skilled team to build and maintain software, you are better served to use a commercial solution. Most often referred to as threat intelligence platforms, or the modern version - threat intel operations platforms.

These solutions allow you to import your own structured and unstructured data as well as commercial / paid, open source (OSINT), and third-party data. Note that open source software is a better option than spreadsheets, but still requires an investment in hosting infrastructure and subject matter expertise to implement and maintain it, challenges that are removed when using a commercial, SaaS-based threat intel platform.

Opportunities for Maturing

Once you have a repository for your threat intel data and you are collecting some OSINT data you should start looking to other free sources of threat information. A great place to begin is with industry peers. There are a number of free communities like information sharing and analysis centers (ISACs) and organizations (ISAOs) that provide industry-specific information about threats, and a secure place for analysts from different organizations to exchange intel and ideas.

MATURITY LEVEL 2 | MANAGED

Warming Up to Threat Intelligence

Analysts at this level focus on threats that come in through alerts. Although it can be difficult to start to work proactively at this level, it is an important step for organizations to start building their threat intel programs. Starting to look beyond reacting to alerts and trying to block threats at the network perimeter, endpoints, etc. using threat intel, like IOCs,is a significant step in the right direction. Organizations also build systems of record for their security program. They no longer rely on spreadsheets and have moved their threat data into a more reliable and accessible system of record, maybe their SIEM, a custom-built tool, or a threat intelligence platform.

Processes and procedures are starting to be formalized and documented in this stage (although tend to be mostly manual). Intelligence requirements are starting to be collected from and vetted by stakeholders to influence the type of intel needed and the outputs required from customers (e.g., operational, tactical, and strategic intel). The first versions of a centralized threat library are established.

MATURITY LEVEL 2 | MANAGED

Recommendations

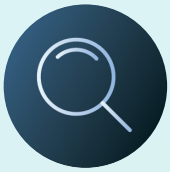
You should begin using vetted threat intelligence. However, many (if not all) organizations have a hard time determining which intel sources (e.g., feeds) are right for them.

Commercial, or paid for, threat intelligence feeds have a range of focus topics and price points. It is recommended that you evaluate feed services providers about how they support your requirements. These are just a few examples of things you will want to identify and evaluate from the provider.

- How timely and relevant is the information, and in what formats is it delivered?
- How much context is included?
- How many false positives does it generate?
- How frequently is the feed updated (hourly, daily, weekly)?
- How well does it integrate with your current security stack?
- How much does it cost?

At this point a feed vendor may have piqued your interest or you may have already implemented your first commercial feed. You will want to trust but verify. Begin to integrate the feed in an evaluation status and see where you can operationalize it.

In terms of your verification process, you will likely want to also periodically revisit the value you are getting from this investment, and adjust accordingly.



Opportunities for Growth

While the aggregated threat data gained at this level is useful, it won't actually provide much context regarding the threats your organization may be facing. For example,

- Is the activity a one-off or is it part of a larger, coordinated series of attacks?
- What information can be gleaned regarding who the threat actors are, where are they located, and what behavior patterns they exhibit?
- If an attack is thwarted, what lessons can be learned and applied going forward?

In order to take the time to start answering those questions, you need one of two things – more people or more time. Skilled staff is hard to come by, so it is important to start looking at developing CTI subject matter expertise and understanding how automation can free up your team's time. Once you start to automate repetitive tasks, you can start considering the questions above. Automation is a key part of growing a threat intelligence operations program.

MATURITY LEVEL 3 | DEFINED

Expanding Threat Intelligence Capabilities

At Level 3, CTI teams proactively identify actionable threat intelligence that addresses the who, why, and how of an attack to draw context and connections and further refine threat knowledge. They are starting to move beyond tactical threat intel and include operational and strategic intel. The use of MITRE ATT&CK is starting to happen so that attacker tactics, techniques, and procedures are being assessed and tracked.

They are taking steps to expand the number of intelligence requirements being developed, tracked, and actioned as part of their standard operating procedure.

They have started to measure intel production and consumption against requirements. Even basic volumetrics like intel volumes processed and indicators supplied to security controls establishes the groundwork for being able to demonstrate the value of the CTI program.

The initial definition and implementation of key use cases, like creating a unified threat library and improving threat detection and prevention, is happening. A threat intel platform is likely being used at this level to implement these core use cases.

MATURITY LEVEL 3 | DEFINED

They have taken steps to start automating certain repetitive tasks, such as data enrichment using Python scripts or a SOAR tool (if it is already being used in the organization).

Instead of spending the bulk of their time on tasks like data collection, parsing and normalization, cybersecurity teams – whether a dedicated CTI team or a small team doing it part-time – have reached a level where data is being turned into knowledge.

It's crucial to maximize the efficiency of analysts at this level in particular and ensure that a team is able to focus on the most pressing and relevant threats. They are collaborating to build and define processes to analyze intel, for example being able to understand an indicator's role in a targeted attack.

Analysts are starting to use visualization tools to amplify analysts' capabilities in analyzing tactical and operational intelligence, for example, using the MITRE ATT&CK Navigator to aid in assessing threat actor TTPs and behaviors. They might be leveraging business data analysis tools to visualize their intel to understand relationships across data points.

At this maturity level, teams take multiple external and internal threat intel data inputs to decipher what's helpful, what's relevant, and what's merely noise, and iterate accordingly. This enables a shift from a reactive to a more proactive posture. In this sense, "proactive" does not mean preventing all attacks before they happen. Instead, what it means is adequately equipping the organization to adapt quickly when an attack occurs, armed with the intelligence needed to fight it.

MATURITY LEVEL 3 | DEFINED

Recommendations

It's at this point that automating tasks in order to keep up with the ever-increasing amount of threat intel data and alerts is necessary. Your organization needs to implement capabilities that can help automate and orchestrate manual threat intel collection, production, and dissemination (e.g., pushing indicators out to security controls)

Automation requires a certain level of trust, so the more information an organization has about threats, the greater the confidence in decisions and automated processes. Because the threat intelligence landscape changes quickly, having access to timely, relevant threat intelligence with minimal false positives is crucial to staying ahead of threats. As you start automating processes, you can start looking into creating your own threat intelligence – an essential part of maturing to Level 4.

Opportunities for Growth

Curb-jump straight to a threat intelligence operations (TI Ops) platform and avoid all the pain of relying on multiple tools (i.e., TIP, SOAR, ATT&CK Navigator, ticketing and case management, Word/Google Docs, wikis, etc) to mature and operationalize threat intelligence activities.

MATURITY LEVEL 4
QUANTITATIVELY MANAGED

An Established Threat Intelligence Operations Program in Place

At this level organizations are starting to build on the operational capabilities achieved so far and establish a structured team approach to strategic analysis. Keep in mind that some organizations may not ever get this level – and that's okay. Not all organizations will have the required resources and funding, or the risk level to justify them. There are ways to improve your program and defenses at every maturity level.

Organizations at this maturity level have well-established requirements, processes and workflows in place, and are even beginning to create their own threat intelligence. As a result, they are creating tactical and strategic CTI, and are automating several analysis tasks.

Having identified persistent threat actors, they are now tracking them and beginning to act on threats more strategically. Multiple commercial threat intel data sources are now implemented. They have joined and are contributing to some ISACs and ISAOs.

MATURITY LEVEL 4
QUANTITATIVELY MANAGED

From a staffing and resource perspective, the organization is also realizing greater efficiencies and increased capacity of the intel team.

Teams at this level need to standardize on a single platform that offers analysts a single pane-of-glass and a unified experience from which to operate. A TI Ops platform is both a system of record and a force multiplier that can help organizations overcome the labor-intensive process of threat analysis that often exceeds the capacity of enterprise organizations. It can handle many of the tasks described above and allow a security analyst to perform many of the sophisticated duties normally reserved for specialized threat analysts. CTI can be quickly visualized and pivoted on to provide a richer picture of threat actors so that action can be taken.

A platform also makes key security controls like SIEM, EDR, NDR, and other security tools significantly more effective and valuable, thanks to the finely curated, relevant, and widely-sourced CTI that the platform enables.

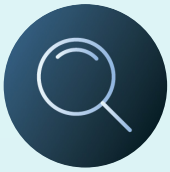
They are improving and increasing the measurements of the efficacy of their processes to report both progress and the impact from investments in the CTI program. Measuring the CTI program is gaining momentum and is moving past volumetrics. Metrics aligned to how TI is supporting stakeholders and impacting the improvement of active cyber defenses are being collected and shared.

MATURITY LEVEL 4
QUANTITATIVELY MANAGED

Recommendations

There is an opportunity for you to move beyond just the tactical use of threat intelligence and use it strategically to inform high- level business considerations; e.g., financial costs of mitigating attacks, brand management, and evaluating ROI on feeds.

If your TI team is operating in a silo, how can they integrate with other facets of the SOC or IR team? It is time to get your entire security operation plugged into a single platform.



Opportunities for Growth

To grow your CTI program you should do more than just aggregate and consume intelligence. You need to be creating your own. At this stage you should memorialize not just IOCs, but context, insights, and knowledge on threat actors. Once gathering and creating this information is part of your processes, your system of record becomes more valuable.

At this stage, your security teams can begin to use historical data to answer questions and inform decision-making. Also, once you have started to create your own threat intelligence, now is the time to ensure that threat intelligence is incorporated into all aspects of your security program. Your SOC can use threat intelligence to better prioritize their events or to determine if they should send something to your IR team.

Your IR team can use threat intelligence to quickly obtain more information about a potential incident and speed up response time. Every aspect of your security team benefits from threat intelligence creation. Once you've done this, you start to look to move to the next level.

MATURITY LEVEL 5 | OPTIMIZING

A Well-Defined Threat Intelligence Operations Program

At the highest level of the Threat Intelligence Maturity Model, organizations have implemented stable CTI programs with formalized processes that are guardrailed with automated workflows and aligned to the Evolved Threat Intelligence Lifecycle. Teams should be producing actionable intelligence and making it available directly to stakeholders, reducing false positives and ensuring rapid, effective responses.

Organizations at this stage disseminate threat intelligence widely, demonstrating and measuring its value in supporting security operations, incident response, risk management, and vulnerability management. AI-driven analytics and automation are integral, enhancing the ability to identify patterns, refine intelligence, and act decisively.

Strategic and operational alignment allows these organizations to effectively detect and respond to threats while using CTI to guide high-level business decisions. Diverse data sources are refined to meet various operational, tactical, and strategic intelligence requirements, supporting multiple use cases.

Codified workflows and automation ensure consistent and efficient threat intelligence operations. SecOps and CTI organizations are aligned and may even share common leadership, each guided by risk-based prioritization from the CISO organization, as well as guiding strategic decisions to help further refine those priorities.

With heavily automated workflows and AI-enabled insights, these teams shift from reactive to proactive, enabling active threat hunting, reductions in MTTR, less impactful incidents, and reduced analyst stress and burnout. This level represents the pinnacle of CTI maturity, where intelligence drives operational security and strategic resilience.

Climbing the Maturity Mountain

As the TIMM shows, achieving an intelligence-driven approach requires people, process, and technology to all be involved. The human aspect of threat intelligence programs is the most important factor.

The investment doesn't have to be huge, and it's important to realize that the most useful sources of threat intelligence are not necessarily the most expensive. Many organizations can start today using existing personnel to improve data gathering and collation. Over time a case can be made to business stakeholders to add automation that would reduce manual processes. Finally, a truly team-driven approach that aligns security strategy with business strategy and the sharing of attack indicators with wider communities becomes possible.

> The problem is getting there. That is where ThreatConnect, the industry's leading AI-powered, Threat Intelligence Operations Platform, can help.

ThreatConnect, powered by its AI and ML-driven analytics engine, CAL™, combines critical capabilities into one cohesive platform. When paired with Polarity, it integrates contextualized intelligence directly into existing tools, enhancing workflows and boosting situational awareness. Analysts can automate threat intel collection, visualize threats with the Threat Graph and ATT&CK Visualizer, capture stakeholder requirements, and streamline efforts with Playbook automation. With native reporting, analysts communicate findings effortlessly. Polarity's federated search, real-time collaboration, and context-sharing enables faster action on insights. Unlike piecemeal solutions, ThreatConnect + Polarity helps organizations advance threat intelligence programs across the TIMM lifecycle at their own pace.

ThreatConnect, powered by its AI and ML-driven analytics engine, CAL™, combines critical capabilities into one cohesive platform. ThreatConnect leverages AI and ML-driven analytics and insights to bridge critical gaps between threat intelligence, risk, and operations. Paired with Polarity - our impactful intelligence and search engine - we integrate contextualized intelligence directly into existing tools and the moment of decision, reducing false positives and boosting situational awareness. Analysts can automate threat intel collection, visualize threats with the Threat Graph and ATT&CK Visualizer, capture stakeholder requirements, and streamline efforts with Playbook automation and workflow. With native reporting, analysts communicate findings effortlessly. Polarity's federated search, real-time collaboration, and context-sharing enables faster action on insights. Unlike piecemeal solutions, ThreatConnect + Polarity helps organizations advance threat intelligence programs across the TIMM lifecycle at their own pace.

ThreatConnect.

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. Over 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

Learn more at www.threatconnect.com.

ThreatConnect.com
3865 Wilson Blvd.,
Suite 550
Arlington, VA 22203
sales@threatconnect.com
1.800.965.2708