

WHITE PAPER

Maturing a Threat Intelligence Program

**Discover the state of your current threat intelligence program
and uncover a roadmap to getting ahead of today's threats.**



www.ThreatConnect.com



The threat intelligence landscape is an emerging one. Even in the most sophisticated security organizations, resource constraints often dictate that threat intelligence (TI) is the responsibility of a sole analyst sifting through incident alerts looking for patterns and trends which may indicate that a threat exists. Threat intelligence is more than that.

Yet, with very little industry standards around what TI is and what it isn't, Gartner's definition^[1] – on the following page – comes the closest to being complete.

[1] Definition: Threat Intelligence. Rob McMillan, Gartner, May 2013 <https://www.gartner.com/doc/2487216/definition-threat-intelligence>

“

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 inform decisions regarding the subject's response to that menace or hazard.¹

Gartner

The Need to Know

Clearly, going beyond simple event-based data analysis is a prerequisite for any useful threat intelligence program.



The problem is that many organizations don't know enough about the threats they face or their own security posture to defend themselves adequately. Instead they're stuck in a reactive or compliance-driven approach to cyber security with no clear vision or blueprint for reaching any other state.

In the rush to keep up with the TI trend, organizations are purchasing standalone solutions that work in silos, making it impossible to achieve a true proactive posture and efficiently orchestrate security solutions and processes to achieve maximum value.

Yet, it's not enough to implement new controls and technologies around systems. In order to fully harness the power of TI, your organization must make the case for an intelligence-driven security approach and identify the right people to staff the program. In order to evolve a defensive posture, 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 both internally between teams and externally with your supply chain partners, peers across the industry, and public organizations.

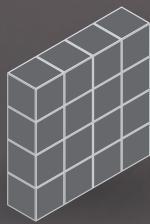
Of course, not all organizations have the resources and organizational structures needed to implement a comprehensive threat intelligence program. And that's fine. Threat intelligence is an iterative process with defined maturity levels and milestones.

ThreatConnect specializes in threat intelligence use cases, so we developed the **Threat Intelligence Maturity Model (TIMM)** more than three years ago with the challenges and opportunities of TI in mind. Whether your organization is just getting started with TI or seeking to expand an existing program, the TIMM provides a systematic guide to see where on the path to a mature threat intelligence program your organization resides; and how to better apply threat intelligence to identify threats faster, drive smarter security processes, and take decisive action to keep a business on course.

The Threat Intelligence Maturity Model

To find out where your organization sits on the **Threat Intelligence Maturity Model**, review each stage and learn about the resources, organizational structures, and technologies needed to achieve strategic processes and operationalize your organization's threat intelligence. The model offers some general direction on the risks and opportunities to grow at each stage, as well as things to consider as you anticipate moving to the next milestone.

THREAT INTELLIGENCE MATURITY LEVELS



••••
MATURITY LEVEL 0
Unclear Where to Start



••••
MATURITY LEVEL 1
Warming Up to Threat Intelligence



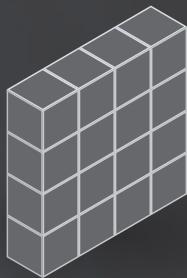
••••
MATURITY LEVEL 2
Expanding Threat Intelligence Capabilities



••••
MATURITY LEVEL 3
Threat Intelligence Program in Place



••••
MATURITY LEVEL 4
Well-Defined Threat Intelligence Program



○ ○ ○ ○

MATURITY LEVEL 0

Unclear Where to Start

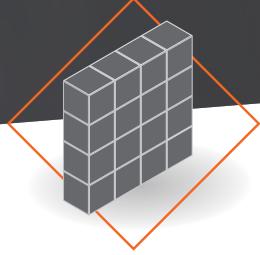
Threat intelligence programs begin life as threat data collection programs. Many organizations start out by seeking external feeds. This can create a new data problem. Where do you put this data? Most organizations keep this information in massive spreadsheets or never-ending email chains, while some feed it into their Security Information and Event Management (SIEM) technology.

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.

oooo

MATURITY LEVEL 0

Unclear Where to Start



TYPICAL TEAM

Not really a team at this stage. The staffing resources needed to support this basic-level threat intelligence program is limited to a security director or network admin.



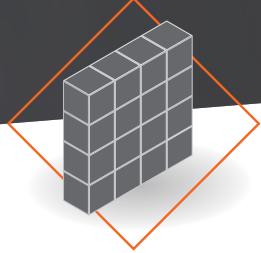
RISKS AT THIS STAGE

Not surprisingly, this stage on the maturity model has room for improvement. If your organization is at Level 0, the TIMM provides an easy-to-follow guide for maturing your program (just keep reading!). The defensive posture between the information gathered and alerting is a labor-intensive and manual process. With added time pressures and many events per day, analyst time spent on each individual event is extremely limited and decisions must be made quickly, often with little to no information beyond what is contained in the alert. Time also adds another element of risk. Due to the manual nature of the work, alerts often point to historical threats and don't account for the fact that adversaries have had time to adapt and try again.

oooo

MATURITY LEVEL 0

Unclear Where to Start



RECOMMENDATIONS FOR NOW

A good place to start involves aggregating internal data and external feeds from multiple sources and cross-referencing it to discover patterns and weed out false positives. Threat data, also known as indicators of compromise (IOC), can then be sent to your endpoint protection devices.

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 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 system of record with a simple database, but there are many arguments against that – the most key of those is bandwidth. Rather than use your limited, highly-skilled team to build and maintain software, you are better served to use a commercial solution as your system of record. Most often referred to as threat intelligence platforms, these solutions should allow you to import your own structured and unstructured data as well as any third-party or OSINT data that you receive. If you do not have budget, look for providers who offer free accounts to get started.

TC Open

TC Open™ is a completely free way for individual researchers to get started with threat intelligence.

You will have access to:

- ▶ 100+ OSINT feeds with new ones being added regularly
- ▶ Ability to look up your indicators of compromise and get more detailed information in seconds
- ▶ Details on active and historic indicators, incidents, and threats
- ▶ Collaboration with peers in communities
- ▶ Research through the Technical Blogs and Reports Source, which is automatically populated with posts from 55 industry blogs carefully chosen by our in-house research team

oooo

MATURITY LEVEL 0

Unclear Where to Start

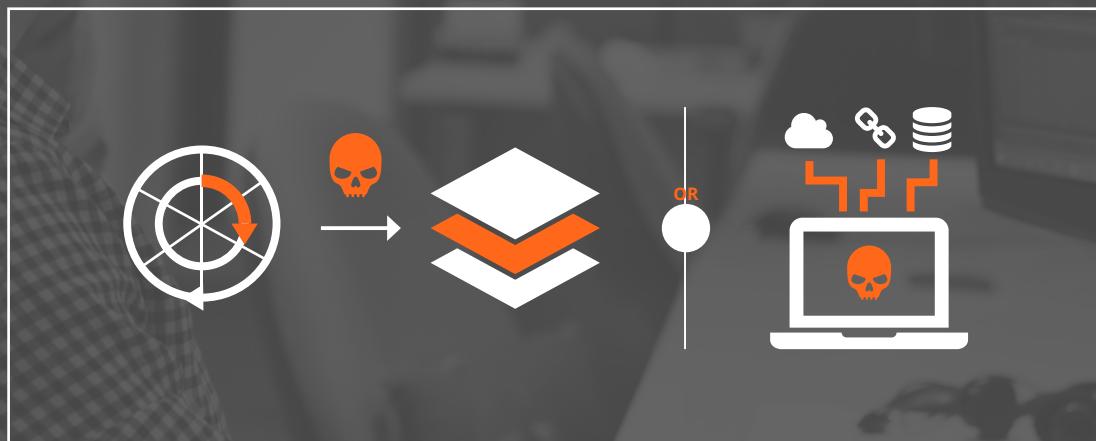


OPPORTUNITIES FOR GROWTH

Once you have a system of record for your own data, your next step should be to look into open source threat intelligence (OSINT) feeds. At this stage, you should already be looking at free, open source threat intelligence (OSINT) feeds. Your team(s) should store that data from the OSINT feeds into a system of record. Threat intelligence platforms and other commercial solutions should convert sources like RSS feeds into machine-readable threat intelligence. Now, your team isn't just consuming intelligence, but can actually use it in your own environment.

Also at this stage, 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 that provide industry-specific information about threats, and a secure place for analysts from different organizations to exchange ideas. Ideally the SaaS platform that stores your threat data should also include secure collaboration – both general and industry-specific.

Once you have done the above, you can start looking into automatically sending relevant threat intelligence back into your environment or exploring premium threat feeds.





MATURITY LEVEL 1

Warming Up to Threat Intelligence

Organizations at this maturity level are beginning to understand and address the massive threat landscape. They are correlating internal data with ingested threat data feeds within their SIEM to begin the process of automated alerts and blocking at the endpoint. Although they have integrated some level of automation into their defensive controls, their analysts likely will be overwhelmed and will experience “alert fatigue.”

Analysts at this level focus on blocking threats that come in through SIEM 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 at alerts and trying to block them on endpoints 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. They most likely use a SIEM, custom built tool, or threat intelligence platform for this step.

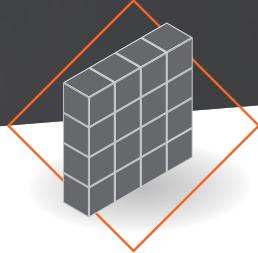
In Level 1, Incident Responders (IR) have similar problems to the threat intel team. It takes too long to detect threats and restore the environment back to a known good state. In order to shorten incident response time, the IR team must focus on improving prevention. The easiest way to do this is for an organization to optimize its current toolset. Every tool, from the firewall to the SIEM to the EDR, should be fed vetted, relevant threat intelligence (ideally from something like a threat intelligence platform). When historic and active threat intelligence is sent to an organization’s tools, it is easier to detect something malicious that has happened in the past.

Using the data gathered in Level 1 in a system of record, an organization can begin to automatically analyze, correlate, and enrich that data to start taking action in their environments.



MATURITY LEVEL 1

Warming Up to Threat Intelligence



TYPICAL TEAM

Network administrator or solo cybersecurity analyst.



RISKS AT THIS STAGE

Although a step forward towards a useful TI program, Level 1 is still a reactive approach with several deficiencies.

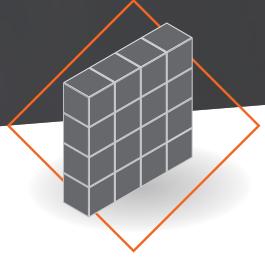
A main limitation of Maturity Level 1 is the SIEM approach. Often, Level 1 organizations depend on their SIEM for all of their threat intelligence needs. However, SIEMs aren't designed to handle the multiple unstructured formats of threat data from numerous sources that are required for analysis. SIEMs tend to quickly become bloated and malnourished, meaning that they get overfed with unvalidated and uncorroborated data, which essentially clogs organizations' security arteries with garbage information. When bad data overwhelms your security posture, you end up losing sight of the real threats to your organization.

Level 1 organizations can't review every single alert, so they hope that the ones they're able to get to with their limited resources end up bearing fruit.



MATURITY LEVEL 1

Warming Up to Threat Intelligence



RECOMMENDATIONS FOR NOW

At Level 1, you should begin looking to start using vetted threat intelligence. However, many (if not all) organizations have a hard time determining which feeds are right for them. ‘Premium’, or paid, threat intelligence feeds have a wide range of focus topics and price points.

It is recommended that you evaluate premium feed providers about how their particular feed supports your requirements. How frequent is the feed updated? How much context on your particular concerns is included? How timely is the information, and in what formats is it delivered? These are just a few examples of things you will want to identify and evaluate from the provider.

At this point a feed vendor may have piqued your interest. You will want to trust but verify. Begin to integrate the feed in an evaluation status and see where you can operationalize it. Is the feed alerting you to the things you care about in a timely manner, or are there too many false positives? Is it updated monthly or hourly? How well does it perform and integrate with your current security stack? 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.

At Level 1, you should start to evaluate entry-level premium threat intelligence providers. Many companies offer threat intelligence that have an approachable price point, either sold a la carte or included as part of a platform.

Once you and your team start to gather some premium intel in addition to the OSINT feeds, you can begin to start gathering context about threats and sending the new information back out into your current infrastructure. Sending vetted threat intelligence strengthens the power of tools like SIEMs and firewalls by ensuring that you are being alerted on the right indicators and reducing false positives – allowing you to find threats sooner.



MATURITY LEVEL 1

Warming Up to Threat Intelligence



OPPORTUNITIES FOR GROWTH

While the aggregated threat data gained in Level 1 is useful, it won't actually provide much context regarding the threat your organization may be facing. For example, is the activity a one-off or is it part of a larger, coordinated series of attacks? And, what information can be gleaned regarding who the threat actors are, where are they located, and what behavior patterns do 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 automation to free up some of 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 mature threat intelligence program.



OR





● ● ○ ○

MATURITY LEVEL 2

Expanding Threat Intelligence Capabilities

At Level 2, organizations proactively identify actionable threat intelligence which addresses the who, why, and how of any given attack to draw context and connections and further refine threat knowledge. They may have taken steps to start automating certain repetitive tasks, such as data enrichment or indicator aggregation. Instead of spending all of their time on administrative tasks, Level 2 cybersecurity teams – whether a small dedicated team or a team doing it part-time – have transcended to a place where data is turned into knowledge. It's crucial to maximize the efficiency of your analysts at this level in particular and ensure that your team is able to focus on the most pressing and relevant threats. They are collaborating to build and define processes that can find what even the most basic indicator's role is in the vast landscape of a targeted attack. To facilitate this level of automation, teams use custom scripts, an orchestration tool, or a threat intelligence platform.

At this maturity level, teams take external and internal data inputs to decipher what's helpful, what's relevant, and what's merely noise, and iterating 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 that organization to adapt quickly when an attack occurs, armed with the intelligence needed to fight it.



MATURITY LEVEL 2

Expanding Threat Intelligence Capabilities



TYPICAL TEAM

To be prepared to handle this level of a TI program, the organization may have a team-based approach, a managed security services provider (MSSP), a small or outsourced security operations center (SOC), or an employee who regularly examines available threat feeds.



RISKS AT THIS STAGE

Threat analysis is often labor-intensive (think sharing incident and threat data by spreadsheets and emails) and TI requirements typically exceed capacity. With attack sources changing by the minute, hour, and day, scalability and efficiency can seem impossible. Large SOCs, for example, produce hundreds of millions of events per day. This is extremely difficult to filter down to a manageable number of suspicious events for triage. Even a couple of unvetted threat feeds going into a SIEM can cause the SOC to become quickly inundated.

Further, without a dedicated TI function, it is unlikely a cybersecurity team has time or the necessary skills for creating its own threat intelligence. So, this team will continue to stay in a reactive mode, addressing only the most visible threats or incidents.



MATURITY LEVEL 2

Expanding Threat Intelligence Capabilities



RECOMMENDATIONS FOR NOW

It's at this point that you must deploy processes for automating security tasks in order to keep up with the ever-increasing amount of alerts. Your organization needs to implement security orchestration capabilities that can automatically analyze the content of threat indicators and the relationships between them. **Security orchestration** allows your organization to automate almost any security task by building out automated chains of events that begin with a specified event in your network. The trick is to ensure that your team is basing automated tasks on vetted and relevant threat intelligence. Tasks that are based on false positives or unvetted data won't save time; just create more work.

For example, an analyst could **automatically** perform relationship modeling on a phishing email to determine who sent it, who received the email(s), which domains it is registered to, IP addresses that resolve to that domain, and so on using security orchestration and threat intelligence. From here, the analyst can pivot further to reveal other domains that use the same DNS resolver, the internal hosts that try to connect to it, and what other host/domain name requests that have been attempted.



MATURITY LEVEL 2

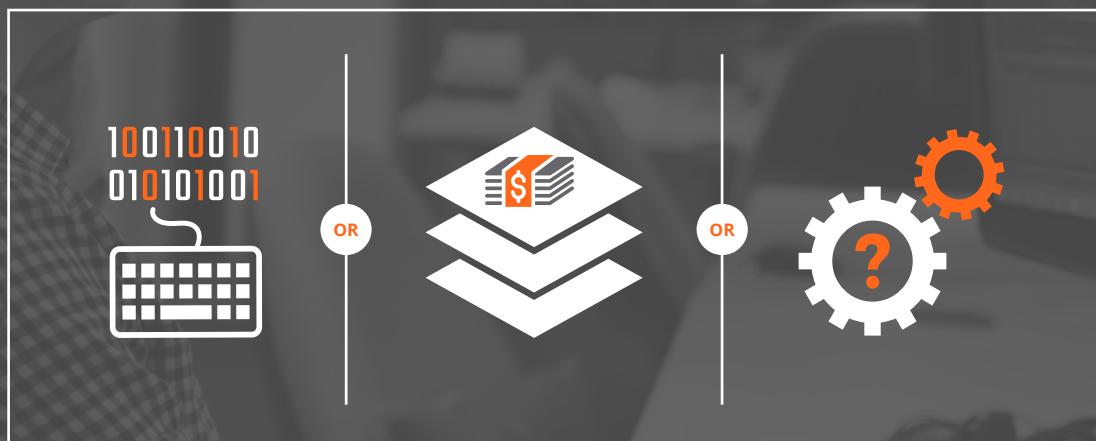
Expanding Threat Intelligence Capabilities



OPPORTUNITIES FOR GROWTH

It is essential that Level 2 teams start to orchestrate some of their tasks or processes. There are a few ways to do this – **have your team start to write custom scripts, invest in an additional automation platform, or determine if your threat intelligence platform has orchestration or automation capabilities.**

It is recommended that you base your processes on the vetted threat intelligence that was mentioned in Level 1. 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 3.



NEED TO JUSTIFY THE COST OF A TIP OR SAO PLATFORM?

Calculate the Savings.

261 = working days per year

\$51/hour = average cost of an analyst

based on a salary of \$91K with \$15K worth of benefits (\$106K total) working 40 hours of week for 52 weeks (2080 hours/year). Actual cost is \$50.96 per hour but we rounded up to \$51.

TIME SPENT ON TASK (measured in minutes)

**X NUMBER OF TIMES TASK IS DONE PER DAY X 261 X \$.85 =
AMOUNT SAVED PER YEAR** by automating that task**

OR

TIME SPENT PER DAY ON THE TASK (IN HOURS) X 261 X \$51

OR

TIME SPENT PER WEEK ON THE TASK (IN HOURS) X 52 X \$51

** Amounts are not exact or guaranteed



MATURITY LEVEL 3

Threat Intelligence Program in Place

It's here at Level 3 that 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 to Level 3 (or Level 4) – 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 some established TI processes and workflows in place and are even beginning to create their own threat intelligence. On top of that, they are beginning to measure the efficacy of their processes to report both progress and security infrastructure health to leadership.

Having identified persistent threat actors, they are now tracking them and beginning to act on threats more strategically. They have joined organizations like Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs).

From a staffing and resource perspective at this stage, this organization is also realizing greater efficiencies and increased capacity of existing intelligence teams. Ultimately, this lowers the threshold needed to establish and reap the rewards of this functionality in existing environments.

A threat intelligence platform (TIP) is a key requisite for this level of maturity. A TIP 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. A TIP 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. TI can be quickly visualized (both by security teams, the organization as a whole, and wider communities) and pivoted on to provide a richer picture of threat actors so that action can be taken.

A platform also drives smarter practices back into a SIEM, intrusion detection, and other security tools thanks to the finely curated, relevant and widely-sourced TI that the platform produces.



MATURITY LEVEL 3

Threat Intelligence Program in Place



TYPICAL TEAM

Typical teams may include the SOC and incident response teams with a security director at the helm; sometimes a dedicated threat intelligence analyst or team may be involved. Network operations and IT staff may also be contributing. Hybrid options also exist in which internal teams handle Level 0 and 1 threat intelligence, while more sophisticated requirements are outsourced to a Managed Security Service Provider (MSSP).



RISKS AT THIS STAGE

The threat intelligence produced by the team will work best when it integrates information from multiple resources and transforms it for use by solutions such as forensics tools, IDS, reputation feeds, SIEM watch lists, etc. Security orchestration may be in place for Level 3 for incident response, but it is likely not fully integrated into end-to-end security operations. So the intelligence being created may not be implemented throughout the entire security process, slowing decision-making.



MATURITY LEVEL 3

Threat Intelligence Program in Place



RECOMMENDATIONS FOR NOW

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 may be time to get your entire security operation plugged into a single platform that integrates with your SIEM, defensive tools, your incident response system, and all internal and external data sources. In doing so, you can create an ecosystem that continues to learn from the actions it takes and adapt to future threats. As an example, if security orchestration resides on the same platform on which your analysts work, they will see the outcomes of the actions taken, be able to examine what is working and what isn't, and use that in their analysis for future actions. Also, your team can document their processes and actions in one place to preserve their knowledge.



MATURITY LEVEL 3

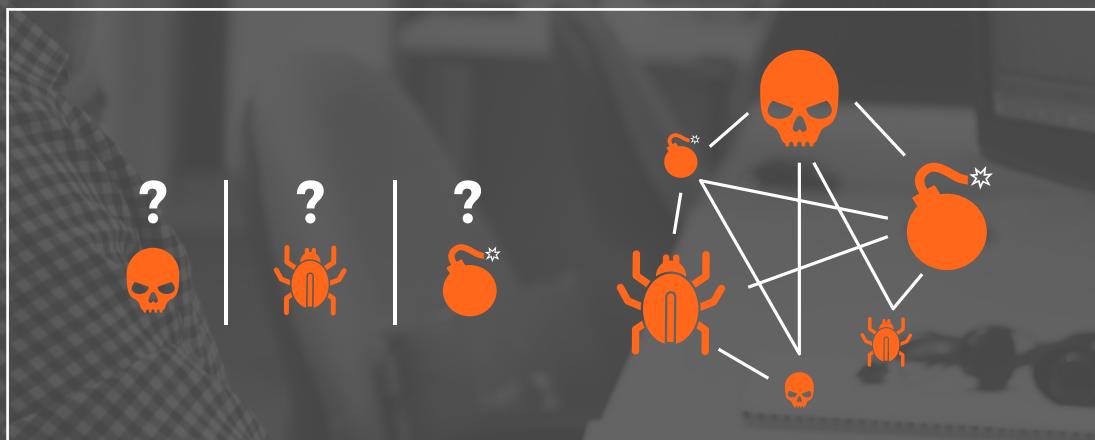
Threat Intelligence Program in Place

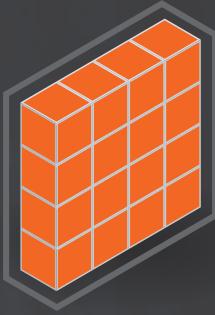


OPPORTUNITIES FOR GROWTH

To grow your program, at Level 3 you should do more than just aggregate and consume intelligence. You need to be creating your own. **At Level 3, you should memorialize not just malicious indicators, but why you consider these actors to be malicious and how they relate to one another.** Once gathering 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 incident response (IR) team. Your IR team can use threat intelligence to quickly obtain more information about a potential incident and speed up response time. Your digital risk team can use the information to determine where threats have indicated vulnerabilities in the past and plan accordingly. Every aspect of your security team benefits from threat intelligence creation. Once you've done this, you start to look to move to Level 4.





MATURITY LEVEL 4

Well- Defined Threat Intelligence Program

At the top of the Threat Intelligence Maturity Model are organizations who have implemented a stable TI program with defined, formalized processes and automated workflows that produce actionable intelligence and ensure an appropriate response.

Organizations at this level typically have a large, mature cybersecurity team that may cover functions such as threat intelligence, incident response, and security operations. Most organizations will have a SOC, and will have made the shift from a reactionary program to that of an intelligence-driven SOC.

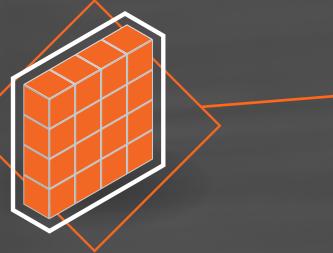
According to Gartner, an intelligence-driven SOC will have the following characteristics: an adaptive security architecture, advanced analytics, extensive automation, proactive hunting and investigation, and will be using threat intel both strategically and tactically.

An organization can't achieve the characteristics listed above or be truly intelligence-driven (a requisite at this level of maturity) without a sophisticated threat intelligence platform that has both orchestration and robust threat intelligence analysis capabilities. Using the TIP mentioned in Level 3, teams can begin to build the Security Operations and Analytics Platform architecture, which allows your developers to build and run their own applications tailored to your unique environment.



MATURITY LEVEL 4

Well-Defined Threat Intelligence Program



In this model, analysts and developers freely share applications with one another, choose and modify applications, and accelerate solution development and task automation through plug-and-play activities.



Teams at this level have built and utilize as much automation as possible, so they have time for more important tasks – like hunting threats. These teams have completely moved from reactive to proactive, and are actively trying to hunt threats before they attack.

Furthermore, **the organization at this level is both operationally and strategically aligned and uses TI to make C-level business decisions**. At this stage, the CISO/security director is using TI to make network and security architecture changes and optimizing security teams that will limit the ability of adversaries to successfully leverage intrusion tactics, techniques, and procedures. The CISO is also reporting on return on investment to prove the effectiveness of the TI program and inform board-level strategic decision-making.



Hitting Threat Intelligence Milestones

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 an element of 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 only intelligence-driven, extensible security platform, can help.

ThreatConnect brings together data analytics, vetted threat intelligence, and orchestration capabilities to provide what an organization needs to build a threat intelligence program. Unlike piecemeal solutions that often only support Level 0 and 1 of the TIMM or closed enterprise software that only the most mature can implement, ThreatConnect helps grow a program across the lifecycle of the maturity model, at an organization's own pace.

BENEFITS OF A MATURE THREAT INTELLIGENCE PRACTICE*

Out of 600 professionals surveyed by SANS, here's what they say the benefits are to their organization:



Increased visibility into threats and attack methodologies impacting their environment



Improved security operations



Improved detection of unknown threats



Improvement in preventing breaches



Reduced time to identify and respond to threats

* Source: "Cyber Threat Intelligence Users, Successes and Failures: The SANS 2017 CTI Survey"





THREAT INTELLIGENCE MATURITY LEVELS



MATURITY LEVEL 0 Unclear Where to Start

MATURITY LEVEL 1 Warming Up to Threat Intelligence

- Aggregate threat data
- Consume threat intelligence
- Use tactical TI to block malicious activity at firewalls or other gateway security devices
- Enhance detection of IOCs as alerts in SIEMs, IDS/IPS, or endpoint protection products

MATURITY LEVEL 2 Expanding Threat Intelligence Capabilities

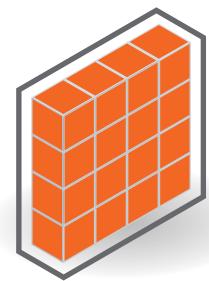
- Produce some operational TI
- Automate some TI analysis tasks
- Leverage TI to triage security alerts and notifications

MATURITY LEVEL 3 Threat Intelligence Program in Place

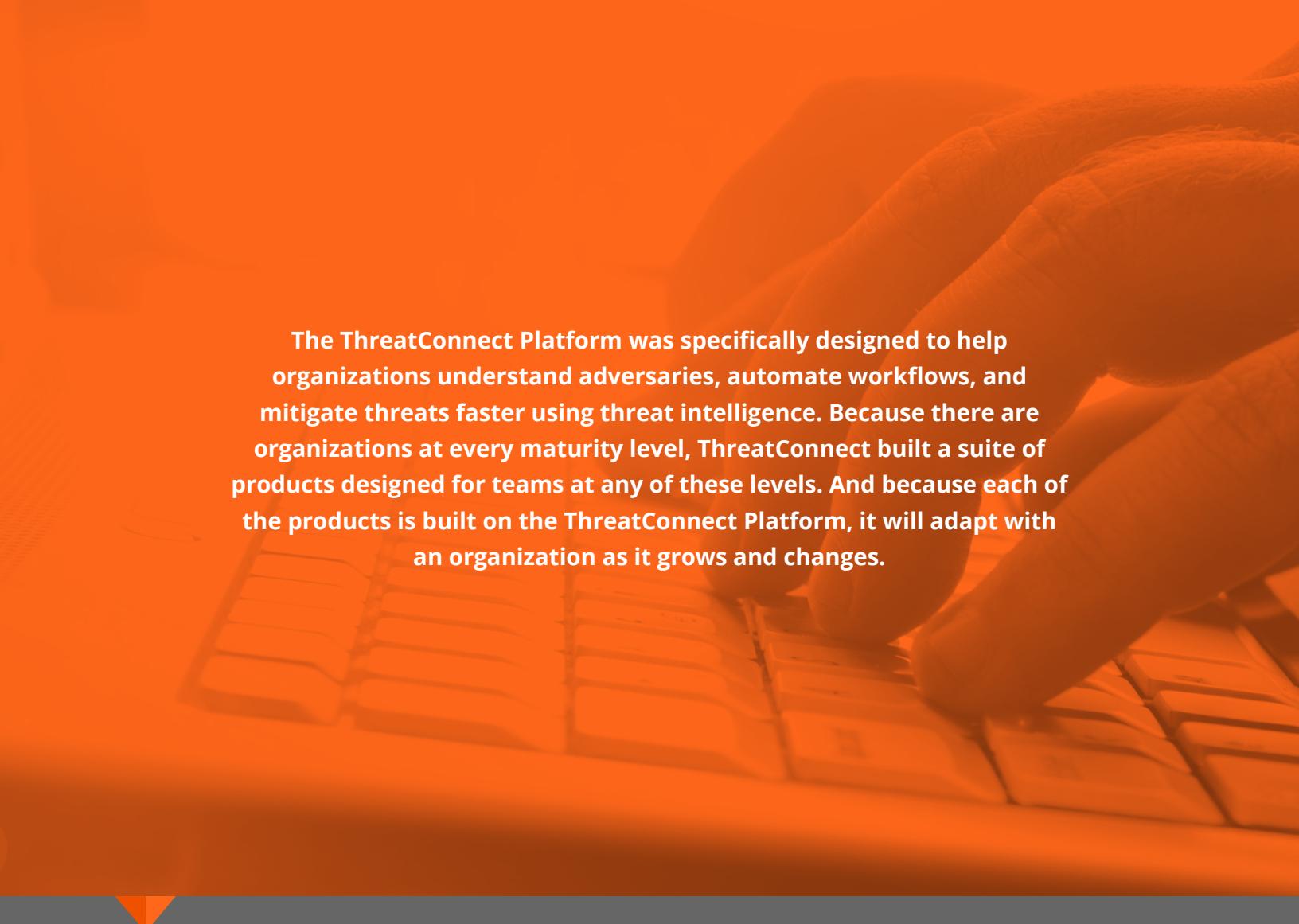
- Some TI processes and workflows
- Create tactical and strategic TI
- Integrate SIEM, defensive tools, incident response system, and all security data in a system of record
- Track persistent threat actors to plan future actions
- Support incident-response processes with TI to prioritize investigations based on knowledge of the adversaries involved

MATURITY LEVEL 4 Well-Defined Threat Intelligence Program

- Mature TI team capable of building custom apps and processes
- Produce and utilize tactical and strategic TI
- Automate as much as possible
- Advanced analytics and orchestration capabilities
- Proactively hunt threats
- Use relevant TI to inform security planning decisions and refine security processes and architecture



The figure above brings it all together. We've defined the key maturity milestones of a threat intelligence program, how and when your organization can achieve them, and how **ThreatConnect can help**.



The ThreatConnect Platform was specifically designed to help organizations understand adversaries, automate workflows, and mitigate threats faster using threat intelligence. Because there are organizations at every maturity level, ThreatConnect built a suite of products designed for teams at any of these levels. And because each of the products is built on the ThreatConnect Platform, it will adapt with an organization as it grows and changes.

Further Reading

TECHNOLOGY OVERVIEW FOR THREAT INTELLIGENCE PLATFORMS (Gartner)

- <https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms>

THE FIVE CHARACTERISTICS OF AN INTELLIGENCE-DRIVEN SECURITY OPERATIONS CENTER (Gartner)

- <https://www.threatconnect.com/gartner>

WHAT'S IN A PLATFORM?

This blog examines how a true threat intelligence platform lets analysts innovate while spending more time on analysis, helps raise the water of threat intelligence for partners, and better serves the needs of directors and the c-suite.

- <https://www.threatconnect.com/whats-in-a-platform/>

SMARTER = FASTER: SECURITY ORCHESTRATION WITH THREAT INTELLIGENCE

This white paper helps you understand how you can make smarter decisions to move faster — both blocking an adversary and disrupting them altogether — by using orchestration with intelligence.

- <https://www.threatconnect.com/wp-content/uploads/TI-Driven-Orchestration-Whitepaper-080917-smallersize.pdf>