ThreatConnect.

Elevating Threat Intelligence to Maximize Impact and Value

The Dawn of TI Ops

Introduction

Threat Intelligence, aka cyber threat intel, has been treated as a "nice to have" for too long. Many times threat intel is viewed as a "check-box" enabled in a security tool. If there is a team dedicated to threat intelligence, it is typically limited to only supporting the SOC with indicators of compromise (IOC) feeds and reports. Often threat intel teams have been relegated to collecting what external intel they can afford or get access to, and writing reports that are sent into a void with the recipient determining relevancy and what action, if any, to take. This leaves the threat intel function and team in a position to justify their value and defend their relevance relative to other security operations functions.

If you are not using threat intelligence and operationalizing it, the adversary wins.

Modernization and digitization of the enterprise, an expanding attack surface, and the increasing dynamism and sophistication of threats requires a more holistic, integrated, agile, and value-delivering threat intel function.

In order for organizations to be more resilient to threats, they need to be more proactive in their response to the most relevant adversaries while working to minimize the exposures that can be used in attacks. Getting ahead of the adversaries requires knowing who they are, their tactics, techniques, procedures, infrastructure, and whether they are relevant to the organization (e.g., industry, geography, software supply chain). Threat intelligence is the critical capability to achieving this forward-leaning position.

To achieve maximum impact, security operations must modernize by adopting a new approach that puts threat intelligence at the core of your security operations function – aggregating threat intel from multiple sources, prioritizing the most dangerous, relevant threats, and proactively taking action. We call this approach Intelligence-Powered Security Operations.

Why? It's Simple.

1. **Focus and relevance:** In order to be highly effective, security teams need to focus on the threats most relevant to their organization, and not worry about every possible threat out in the wild - which would wastes already limited resources with little benefit. Focus can be realized with actionable knowledge of the capabilities, tactics, infrastructure, and motivations of threat actors provided by relevant, high-fidelity threat intel.

2. **Proactive and responsive:** The ability to take timely action on accurate and relevant threat intel allows security operations teams to anticipate and get ahead of attacks, proactively improve their defenses, and respond quickly and more precisely when they are attacked.

The Dawn of the TI Ops

This new approach, called Threat Intelligence Operations (TI Ops), has been increasingly adopted by leading edge organizations who have seen dramatic gains in key measures of security effectiveness - faster time to mitigate critical vulnerabilities, and faster mean time to detect (MTTD) and respond (MTTR) to the most relevant and critical threats.

The Tenets of Threat Intelligence Operations

There are seven tenets that define and position TI Ops. These are:

1. Elevates threat intelligence to a mandatory, critical security operations role.
2. Requires an Evolved Threat Intelligence Lifecycle, one that emphasizes the planning and requirements and the use of threat intel by the consumers.
3. Threat intel is aligned and focused on the most critical risks to the business through a living set of requirements.
4. Focus is not solely on indicators of compromise, but expands to cover the motivations, tactics, techniques, trends, tools, and infrastructure patterns of threat actors.
5. Automates the work of the TI Ops team.
6. Integrates and automates threat intel into every aspect of security and cyber risk management.
7. Creates measures of effectiveness and success for produced and consumed threat intel that are understandable and relevant to the business.

The Elevation of the Threat Intel Team

People are the heart of a TI Ops team. Analysts are the glue between the processes and the tools. Analysts enact, refine, and optimize the threat intelligence operation tradecraft. However, the current reality is that many CTI teams are not ready to evolve into a TI Ops team.

A 2022 survey by ThreatConnect showed a majority of TI analysts ranked Collection and Processing as the activity they spent the most time performing. This is problematic because the survey also highlighted that analysts strongly prefer to be spending their effort on Analysis and Production! Analysts understand that time spent on those activities is their best opportunity to make the biggest impact. Unfortunately, they report being slowed down in Collection and Processing by low-quality data, integration issues, and especially by manual tasks.

When TI Ops is placed at the core of security operations, the TI Ops team has to step-up to the challenge of being given more visibility, responsibility, and criticality. They must elevate what they do and how they do it.

- They need to ensure there are agreed and documented requirements. Not having requirements impacts how relevancy, value, and success are measured.
- They have a customer-centric mentality and approach to threat intelligence ensuring that they are producing relevant, high-fidelity intel appropriate to their customers' and consumers' needs and requirements, at the right time and in the right format.
- TI Ops teams must embrace automation across the aggregation, enrichment, analysis, and action phases of TI Ops. Any manual work slows down processes and removes analysts from focusing on the work that matters.

Results from conversations and surveys of threat intel analysts and leaders confirms that their goals are to be more strategic rather than in firefighting mode, provide valuable threat intelligence to customers, and make an impact for their organizations. Embracing a TI Ops approach makes these goals achievable.

The Evolved Threat Intelligence Lifecycle

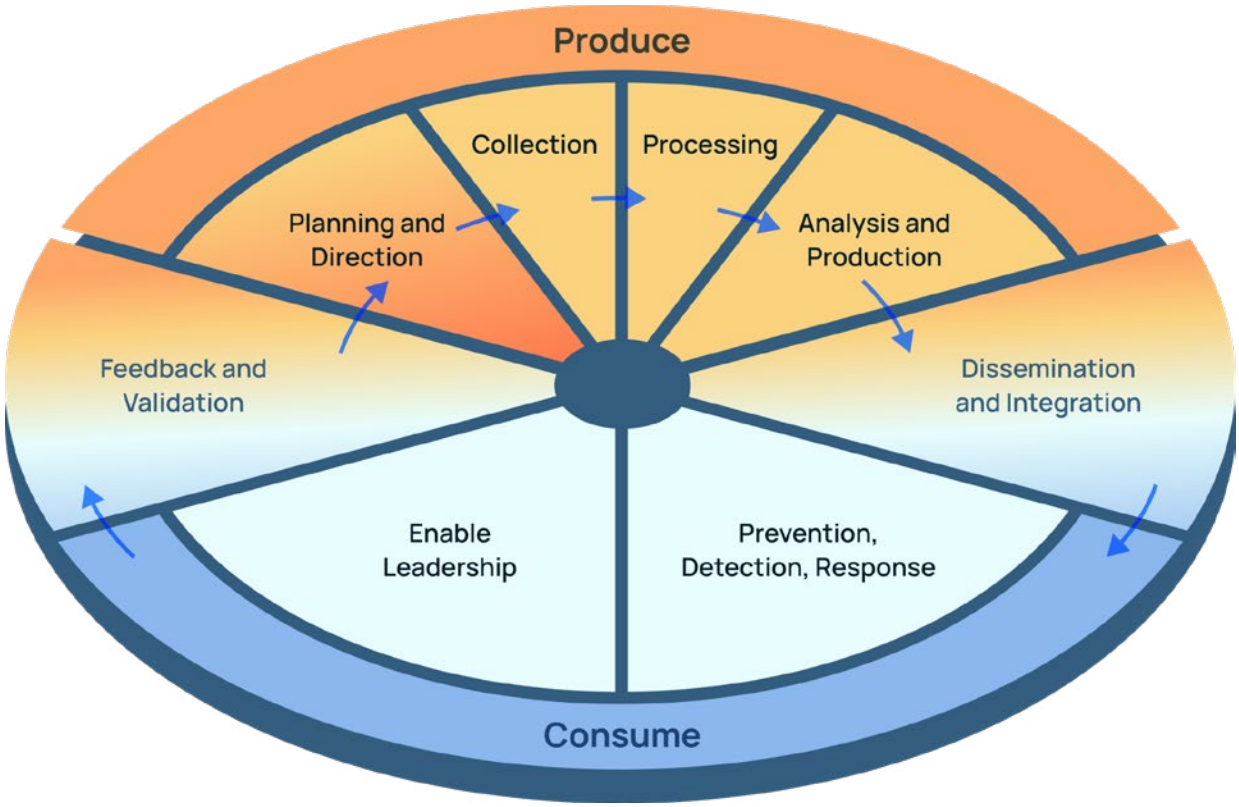
The cyber threat intel lifecycle has been a reference point for nearly two decades, but as threat intel has gained broader acceptance and adoption, the cracks are starting to show. We believe it's time for an evolution of this lifecycle.

TI Ops requires an Evolved Threat Intelligence Lifecycle, one that emphasizes the **planning and requirements and the use of threat intel by the consumers** to create a complete view of what threat intel is needed to align and focus on the critical risks to the business, support other security operations functions in a collaborative manner, and identify how it can best deliver that intelligence to the right teams, in the optimal format, at the right time.

In order to evolve threat intelligence (and threat intelligence analysts!) from a nice-to-have to an essential component of a security team, we need to unpack two key weaknesses of the intel cycle:

1. **Insufficient Consideration of Intel Consumers (i.e. Stakeholders)** - Threat intel has a purpose! It's created in order to help leaders make smarter decisions, help the SOC reduce false positives and improve detection efficacy, inform red team activities, kick off more relevant threat hunts, and so much more. Those stakeholders are key components of helping an intel program evolve, but the intel cycle leaves them out, essentially ending with "Dissemination and Integration" as though once intel created it's handed off into a void, rather than part of a continuous, collaborative feedback loop.
2. **Lack of Formalized Feedback and Measurement** - "Feedback" and "Evaluation" encircle the old intel cycle. Each step in the process should be continually assessed for opportunities for gains in efficiency and effectiveness. However, in order for threat intel to be seen as essential, there needs to be clear and quantitative evaluation with strong participation from the stakeholders. Intel teams put a lot of time and effort into the intel they produce, and they're proud of it.
    - Did it help reduce false positives? Improve detection efficacy?
    - Were recommended actions taken, and did they have an impact?
    - Was a strategic report found useful by the CISO?

Intel teams not only need to support their stakeholders in assessing these metrics, the stakeholders need to understand their role in closing the loop.



The Evolved Threat Intelligence Lifecycle is divided into three key areas:

- **Produce** - This represents the bulk of the classic intelligence cycle and focuses on the activities involved in actually creating new intelligence (or making existing intelligence digestible to new audiences).
- **Consume** - This is a new addition to the intel cycle. Instead of the cycle "ending" at the handoff, we explicitly call out the stakeholders: the teams and tools we're actually creating the intelligence for.
- **"Bridge" Steps** - Rather than being part of Production or Consumption, Dissemination and Feedback are the bridges between the two and are intended to be collaborative efforts.

By recognizing both Producers and Consumers, the Evolved Threat Intelligence Lifecycle brings in all parties involved in threat intel, and the bridge steps bring them together in a way that encourages accountability. In other words, it enables the value threat intel brings to be clearly communicated across and up. Let's take a look at the steps in the cycle in more depth:

1. Produce

- **Planning & Direction** - Starting with a **well-informed plan** and **priority intel requirements** (PIRs) that are aligned to the needs of the business is critical to all other steps. When the loop is closed on the cycle, this step heavily incorporates feedback from Consumers: was the needle moved for key metrics like MTTR or false positive ratio? Was the intel presented in such a way that it enabled solid decision-making? How might we improve?
- **Collection** - From **OSINT** and **paid feeds** to your own telemetry, collecting from sources both broad and deep provides a solid foundation. Much of this collection can be **automated**.
- **Processing** - Separating the wheat from the chaff starts with **standardized**, **normalized data** that can be correlated with other **memorialized intelligence**. **Automation** and **analytics that can help enhance data quality** are essential at this step to free up analysts to spend more time on Analysis and Production.
- **Analysis & Production** - This is where analysts should be spending most of their time and where they can have the biggest impact. **Automation** can speed a lot of the grunt work while global, crowdsourced insights and analytics from other analysts can help improve **accuracy**.

2. Dissemination and Integration - Whether via **reports**, **APIs**, **visualizations**, or **external sharing**, the value of all the hard work up to this point depends on getting the right intel to the right people at the right time.

3. Consume

- **Prevention, Detection, Response** - Key stakeholders like **SOCs**, **fusion centers**, **IR**, v**ulnerability and exposure management**, and other teams depend on intel to **tighten defenses**, **improve detection efficacy**, and **speed response**.
- **Enable Leadership** - Leaders from the **CISO** on down need to be enabled to make sound decisions and take informed action. **Automated reporting** can ensure the right intel, **metrics**, and **KPIs** are swiftly and effectively communicated.

4. Feedback and Validation - Feedback needs to flow through everything. Is the intel moving the right needles, or is your team inundated with **false positives**? Are your reports **driving action**, or getting ignored? Feedback also informs future planning efforts. Getting this step right may be the most essential element of the new cycle towards making threat intel a must-have.

Teams are only as effective as the mental models they use to drive their work. By applying the Evolved Threat Intelligence Cycle, threat intel teams can have a bigger impact, grow their expertise, get more budget, and ultimately be the heroes to the broader organization that they want to be. Mental models, though, are only as effective as the tools that can be brought to bear to realize them. That's where the TI Ops platform comes in.

A Unifying Threat Intelligence Operations Platform is Required

TI Ops utilizes a combination of human analysis, machine learning-powered analytics, automation, and integrations across the security team's tech stack to radically increase the effectiveness of threat intel analysts and security operations teams. By bringing together previously siloed tools and teams, TI Ops focuses the entire team on the highest priority threats to deliver maximum effectiveness and impact.

A TI Ops approach also continuously measures the effectiveness of the CTI function overall, for example -

- How well did it impact security operations key performance indicators? (MTTR, MTTD, etc.)
- How timely, accurate, and relevant was the intelligence provided to stakeholders?
- Did it highlight detection or prevention gaps for the security operations team?
- Was it able to provide early insight into an adversary targeting one of your business-critical suppliers?

This allows for refinement and improvement of collections, analysis, and resource allocations to align to the needs of the organization.

However, the current tools and approaches are inadequate to enable and support TI Ops. They rely on manual analyst efforts and siloed tools and teams. Spreadsheets and legacy threat intel platforms cannot flex and scale, and lack robust, easy to use automation. Measures and metrics are qualitative and expensive to collect, making it difficult to articulate the value of CTI.

TI Ops requires their own platform. An apt corollary are business intelligence (BI) tools. These solve similar challenges for teams like business operations, marketing, finance, and process management. They address big data challenges. They transform raw data into something usable for analysis, enabling insights and value to be extracted from the data. A TI Ops platform does the same thing for CTI.

"Threat intelligence platforms are still not the main tool used by CTI teams—not in the top four—with 'spreadsheets/ emails' leading the way once again, while one out of two respondents still prefers homegrown CTI platforms."
– SANS 2022 Cyber Threat Intelligence Survey

SANS 2022 Cyber Threat Intelligence Survey

The Critical Capabilities of a TI Ops Platform.

A TI Ops platform requires modern capabilities. Beyond just providing raw data like a feed or SOC-focused automation, like a SOAR tool, it needs dedicated tooling to help TI Ops teams and their stakeholders get their job done. Augmenting analysts with machine power is now the norm. Without these, the mission of the TI Ops team will not be achieved.

- **AI and ML** - Applying machine intelligence to threat intel is not a nicety. It's necessary. Machines scale, and can work faster and discover insights that take humans much longer to uncover (if at all). This is a reality and a benefit that needs to be embraced, not dismissed. Machine learning is baked into many security tools now. It's become the norm, not the exception. AI techniques, such as natural language processing, are following on the heels of ML. Find opportunities to leverage these capabilities to supplement the more tedious steps like Collection, allowing analysts to focus on high-value activities like Production.
- **Automation** - Analysts are expected to go fast and be efficient. However, humans struggle to multi-task and maintain focus over long periods of time. This is the reality. Automation is a game changer across TI Ops, much as it has become across modern security operations. Automation comes in many forms, whether it's automating a simple task an analyst performs multiple times per day, like enriching an indicator, or automating a complex, end-to-end process like analyzing a suspicious phishing email and reacting to its purpose and maliciousness. If an activity can be automated, a TI Ops platform should make it happen. Note that not all automation tools are created equal: what works for a SOC, IR team, or even sales and marketing team won't always meet the needs of a dedicated TI Ops team (at least not without a lot of customization).
- **Visualizations** - Some analysts like their data in tables, others want their data visualized, many want both. Being able to "see" threat intelligence data in a way that analysts can interact with the data is needed. Just as BI tools present data visually, so must TI Ops platforms. This allows analysts to gain a rich understanding of the data, pull on threads to see where it takes them, understand the connections and linkages across different types and points of data, and memorialize their findings. More than just "pretty pictures" these visualizations should both help analysts uncover insights as well as tell a strong, high-integrity story to their stakeholders.
- **Access Threat Intel Data Anywhere** - If threat intel is only accessible to analysts within the confines of a platform, then its value is not going to be fully realized. Making threat intel accessible to other teams and analysts when they need it, like when they are using a SIEM or a vulnerability management tool, is more efficient (e.g., not having multiple console windows open, copying and pasting across screens) and generates more usefulness and value. Conversely, if TI Ops analysts have to do the same motion – multiple consoles open, copying and pasting between screens – then their work and efficiency is impacted. Being able to quickly memorialize new threat intel into their TI Ops platform liberates them from these inefficiencies.
- **APIs** - These are the modern glue between applications. Without a robust, highly functional API, any platform cannot be considered modern (or even that functional). A TI Ops platform must be able to easily integrate upstream and downstream sources to support TI Ops' mission and realize the value from their intel.
- **Reporting** - Presenting insights to others is an important output for TI Ops, e.g. for sharing strategic, tactical, and operational intel. Manually producing reports is a tedious and time wasting process. Again, a business function would never buy a BI tool without a robust reporting capability. TI Ops teams should have the same expectations for their core work platform. A TI Ops platform must have a WYSIWYG reporting capability to make report writing and sharing fast and easy.
- **PIRs** - The Intel Cycle starts with planning. Being able to define, track, and measure Priority Intelligence Requirements helps ensure that teams are focused on the most relevant threats to their business. PIRs are the universal language that help map business priorities to threat intelligence activities.
- **Metrics** - It's often hard for CTI teams to understand the impact their intelligence is having: is it reducing false positives? Improving detection efficacy? Lowering risk? Helping leaders make sound decisions? In order for threat intel to become an essential element of a security organization, TI Ops needs to help analysts quantitatively measure the value of their intel and answer questions around whether it's moving the needle. In addition to showing the value of threat intelligence, this also helps CTI teams continuously improve their own processes.

Your Next Step

Security leaders MUST elevate the TI Ops team to their rightful place - at the center of security operations. Those who adopt and enable TI Ops will achieve (1) the needed alignment between security operations and the critical risks to the business; (2) better security efficiencies AND greater effectiveness; and (3) measurable and demonstrable value for TI Ops and security technology investments.

Reach out to learn how the ThreatConnect Platform can make you and your team more effective, decisive, and collaborative.

+1 (800) 965.2708 -or- **ThreatConnect.com/Request-a-Demo**

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. More than 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203
sales@threatconnect.com
+1 (800) 965.2708