ThreatConnect.
now a part of Dataminr

Whitepaper

How the right platform makes operationalizing cyber threat intelligence a game changer for security operations

# Modernize Your Threat Intelligence Platform

# Introduction

Perhaps the greatest challenge in the whole of cybersecurity operations is the asymmetric information that's inherent to the field. After all, organizations – regardless of whether they're publicly-held companies, privately-owned corporations or partnerships, government agencies, or non-profits – exist in the public realm. They're registered entities, and information about their structure, makeup, and purpose is readily discoverable. Adversaries conduct in-depth research about their targets relying only on sources that are publicly available.

Attackers, on the other hand, exist within a shadowy underworld realm that's clandestine, difficult to break into (or even learn about), and fluid.

This means that attackers will always know more about their targets than defenders know about their adversaries. What's more, no one can ever be confident that they understand the size and scope of the threat landscape and actors, which is accelerating.

**Attackers will always know more about their targets than defenders know about their adversaries.**

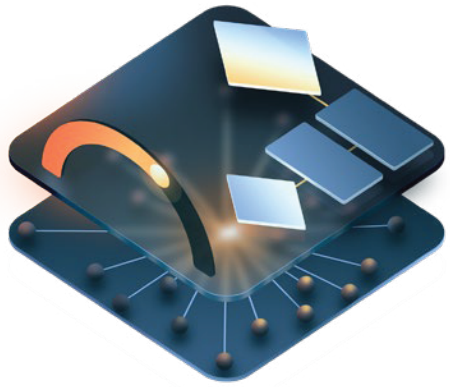
Cyber threat intelligence and operational information-sharing can help **right the balance** of power between attackers and defenders.

Criminal activity tends to trend up every year, but it escalated in unprecedented ways as the COVID-19 pandemic spread across the globe in 2020. Research conducted by the Information Systems Security Association (ISSA) and the Enterprise Strategy Group (ESG) reveals that defenders confronted a 63% increase in overall attack volumes in the immediate aftermath of the pandemic's outbreak.[1]

2021 also saw a dramatic increase in ransomware attack volumes, and ransomware was responsible for a 25% of the data breaches examined in Verizon's 2022 Data Breach Investigations Report (DBIR), an increase of almost 13% from the previous year.[2]

In total, ransomware victims paid out approximately $350 million worth of cryptocurrency in 2020, a 311% increase from 2019.[3] Nation-state attackers became morebrazen during the same period, with research indicating that 'significant nation-state attacks' increased by 100% from 2017 to 2020, with attacks becoming more frequent and attack techniques more varied.[4]

According to David Shearer, CEO of the International Information System Security Certification Consortium, or (ISC)[2], today's defenders are simply "outnumbered – the people that are doing bad things, whether it's nation-state type activity or cybercrime – the good guys and girls were vastly outnumbered even prior to the pandemic. [The pandemic] had a compounding effect on what was already a challenge…take all of this technology we are becoming more reliant on and [this challenge] is scaling at a massive pace."[5]



1 The Impact of the COVID-19 Pandemic

2 The 2022 Verizon Data Breach Investigations Report (DBIR)

3 Ransomware 2021

4 Nation States, Cybercrime, and the Web of Profit

5 Quotes in "We are outnumbered"

Approximately 2.8 million professionals currently work in the cybersecurity field worldwide, but an estimated 3.1 million roles would need to be filled to meet demand, close the skills gap, and adequately protect organizations.[6] Still, these numbers are only estimates. And there's simply no way of telling how many individuals participate in cybercriminal activities or engage in cybercriminal networks. We can be confident that attackers and defenders aren't evenly matched, but we can't be sure how great the imbalance is.

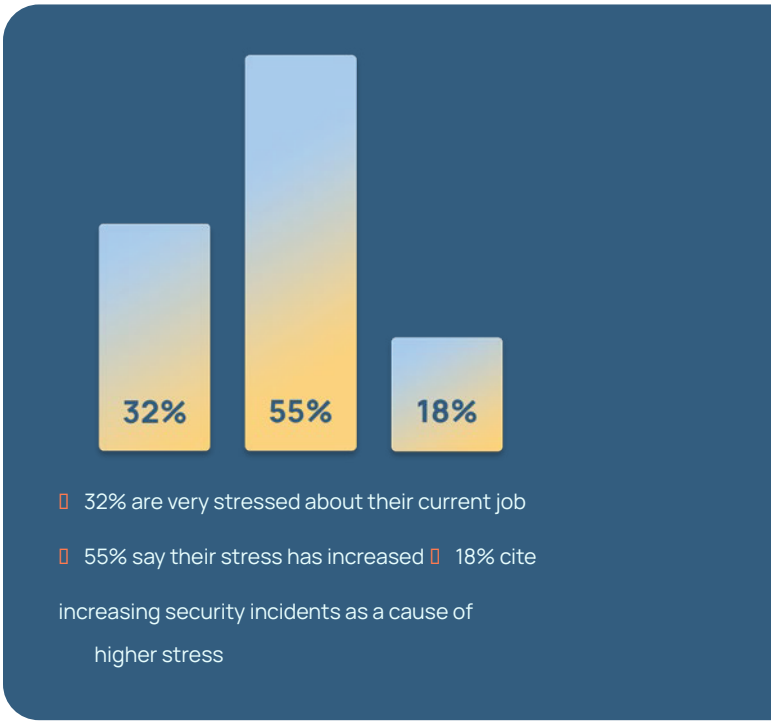
It's clear, however, that the demands on today's security operations (SecOps) and SOC teams are greater than ever. A recent study by us revealed that 32% of security workers report being very stressed about their current job, and more than half (55%) say their stress level has increased in the past six months. The most common causes of stress are heavy workloads, long hours, and tight deadlines. Further, 18% reports a rise in security incidents as another major cause of stress. [7]

In the face of challenges that cybersecurity teams currently confront, it's more important than ever that they're able to use all of their resources – including knowledge, tradecraft, creativity, and analytics skills – as effectively as possible. There's an enormous need for solutions that will enable them to maximize their potential.

When it's properly applied and integrated within an enterprise-grade security program, that's exactly what cyber threat intelligence (CTI) does.

6 (ISC)² Cybersecurity Workforce Study

7 ThreatConnect Report – CyberSecurity Under Stress



# How Cyber Threat Intelligence Acts as a Force Multiplier for Highly Effective Security Operations Teams

On average, an enterprise SecOps team investigates only 48% of the alerts that it receives. Among these, only 26% are found to have any value or legitimacy whatsoever.[8]

CTI gives security teams a means for assessing whether alerts or events are meaningful within the context of broader situational awareness. This enables analysts to train their attention on the greatest threats that their organization faces at any particular time.


On average, an enterprise SecOps team investigates only **48% of the alerts** that it receives

Providing access to aggregated CTI data from commercial, open source, government agencies, private enterprises, and independent security researchers – all consolidated, normalized, deduplicated, enriched, prioritized, and maintained in a single centralized threat library – high-quality CTI acts as a lens to better understand the outside threat landscape.

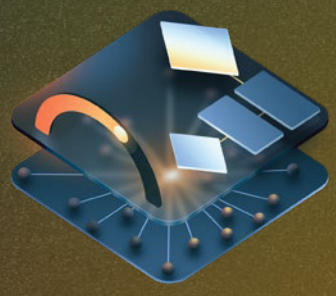
CTI allows SecOps teams to act more quickly and decisively, by informing them who adversaries are targeting, how adversaries act (i.e., their tactics, techniques, and procedures), and what tools they tend to use. This enables analysts and incident responders to better understand and defend against the adversary during all phases of an attack.

CISO Benchmark Study 2020[8]

## To be most effective, cyber threat intelligence must be actionable.

This means that it can be used as a basis for tactical and strategic decisionmaking. If it is to be actionable, it must be accurate, relevant, and aligned with your organization's characteristics.

Actionable cyber threat intelligence should also be applied through wellintegrated tools and solutions. Seamlessly integrating intelligence into operational and strategic activities, and leveraging automation, helps decrease security teams' stress and workload, and reduce risk to the organization.



01

# What is Cyber Threat Intelligence? Why does it Matter?

CTI is the collection, investigation, and analysis of data about an adversary's motives, goals, tactics, techniques, procedures, weapons, and infrastructure.

This information can give security operations teams a holistic picture of the threats they face – one that can be applied within the operational and strategic defense of computing resources. This knowledge better enables an organization to detect, understand, and defend against attacks.

# Threat Intelligence Management

Threat intelligence management needs a platform, aka a TIP, that consolidates information from multiple threat intelligence sources, such as feeds, information sharing, reports, blogs, and other sources into a single location where it is processed and made usable for machine and human analysis. They help make CTI usable and actionable. Humans can rely on it as a knowledge source to draw upon when analyzing and responding to incidents, and automated tools can act on the real-time data it provides.

A well-designed and executed TIP transforms what would otherwise be decontextualized data into highly relevant insights. The TIP thus gives security teams a holistic view of threats, adversaries, and tradecraft in their current state. And it lets them understand how thecyber threat landscape is evolving – in real time. Incorporating a TIP into your security operations team can improve your detection, prevention, and response capabilities. It provides actionable intelligence that can guide alert triage, incident response, and proactive threat hunting activities, and can be a catalyst for bolstering your cybersecurity defenses. It can also help teams prioritize where to invest their efforts, and can guide business decision-makers in evaluating risk.

However, for a TIP to be implemented successfully, there are several preliminary steps that should be taken. Unfortunately, many businesses jump straight into purchasing a TIP without doing the preparatory work, only to find that the "solution" doesn't solve their problem.

# CTI is derived from two types of sources:

**1) Internal Sources:** These are sources retrieved from your own network and computing environment. Internal sources include log files, alert histories, incident response reports, and network and security tool telemetries. Many security teams leverage a Security Information Event Management (SIEM) solution as their primary repository of internal threat data. Adding details from past incident response processes – such as which systems were impacted, which vulnerabilities were exploited, and which malware was employed – can increase the maturity of your internal threat awareness program. Internal systems often reveal the threats that are most relevant to your organization on an individual basis.

**2) External Sources:** There are a wide variety of external CTI sources to choose from. These include open-source and commercial threat intel feeds as well as blogs written by security researchers and vendors and publicly available reputation and block lists. Besides intel feeds, private or commercial sources of CTI can include structured data reports, unstructured reports, and informal sources (such as an email message from an industry expert). Often, the challenge with this wealth of data is to determine its relevance as well as to refine it with context to ensure that it's actionable within your organization's unique threat landscape.

# Building an Effective Threat Intelligence Operations Function

## First, establish your intelligence requirements

Everyone knows that no two businesses are exactly alike.They have different missions, audiences, products, financial underpinning and, of course, risk profiles that can be informed by threat intelligence. Unfortunately, there's no shortage of sources – in fact, it can seem like there are far too many! The poor analyst who is faced with an increasingly complex threat landscape, and a barrage of threat intel data, can be overwhelmed.

That's why it is vitally important to establish a set of requirements (usually referred to as Priority Intelligence Requirements, or PIRs) as afoundation for managing threat intelligence and operationalizing that intelligence in a tool, with a goal of enabling Threat Intel Operations (TI Ops) teams to process threat data into intelligence.

The exercise must start by identifying the critical assets and prioritizing those that make your business a target. For each, evaluate the relevance of potential threats. There may be other similar businesses that have had their assets targeted, or you may have been the target yourself. Focus on PII, financial information, authentication credentials, and other types of data that are frequently targeted.

## Armed with a clear understanding of your intelligence requirements, take a look at the primary functions that threat intelligence can serve:

**Operational:** Threat intelligence with operational functionality is used to increase detection capabilities as well as to help teams identify the vulnerabilities that are most likely to be exploited. Technical CTI activities focued on specific threats and indicators (IoAs, IoCs) and artifact analysis, malware analysis, enrichment, and behaviors, and intelligence dissemination.

**Tactical:** Focuses on attacker tactics, techniques, and procedures(TTPs), tools, and infrastructure. This intelligence is leveraged to optimize cyber defense activities.

**Strategic:** Strategic threat intelligence can help business, technology, and security leaders understand the size and scope of current and future financial, reputational, and operational risks that the organization faces. This information typically outlines the organization's exposure to particular threats as well as the status of the organization's assetsand revenue streams. Strategic threat intelligence can be gathered through threat assessments, critical business process mapping, and quantitative risk analysis.

When contextualized, strategic, tactical, and operational threat intelligence is fused into and across all SecOps functions and activities it becomes optimally effective, enabling decision making based on current situational awareness and historical patterns.

# Second, Recognize that Not All Intelligence Sources are of Equal Value

After all, detailed data about the tactics, techniques, and procedures employed by an adversarial group that's no longer active aren't terribly useful, and worst case can create false positives that can waste time for other teams. Nor is information about exploits targeting a vulnerability in software that's not deployed anywhere in your environment.

**In order to evaluate a particular threat intelligence source, you'll need to consider its merit within each of the following categories:**

**Relevance:** How well does this source help you understand the threats that are most relevant to your individual organization? This relates closely to the assets defined in the IR section above. You will want to map your business processes to specific geographical, political, and industry-focused threat types. This will help you understand which are most likely to target you. In actuality, determining a threat intelligence source's relevance is an iterative process. The more you learn about the unique and specific risks that your organization faces, the better you can understand which intelligence is most relevant to your threat profile.

**Timeliness:** How frequently and rapidly is the feed or source updated? And how does this frequency compare to the frequency of changes in the threat landscape? Some types of threat intelligence are more subject to change than others; this is largely dependent upon adversaries' skills and resources. If a threat intelligence source provides a way to detect adversarial activitythat persists despite the evolution of those adversaries' capabilities and infrastructure, that intelligence won't need to be updated as frequently. In general, though, feeds and sources that evolve rapidly to reflect changing adversarial capabilities are best.

**Accuracy:** How often does this source create or contribute to the creation of false-positive alerts? How well does it reflect the true state of adversarial capabilities today? And how well does this intelligence help analysts and incident responders understand the critical context surrounding their decisions? Accuracy is reflected not only in confidence ratings or certainty scores, which are evidence of the source's fidelity to the real world, but also in the information's usefulness for helping members of your team figure out which steps to take next when they confront an alert. Accurate threat intelligence enables incident responders to direct their efforts where they'll matter most, and can help both TIOps and security operations analysts to understandthe motives and capabilities of their adversaries

**Variety:** How broad is the array of endpoint- and network based indicators or signatures that this source leverages? Across how many phases of an intrusion or attack lifecycle is the information relevant? The more indicators or detection techniques employed, the better. The more relevant, timely, accurate, and varied the threat intelligence source is, the better it will be able to fulfill its primary purpose – to empower security teams to take the right action at the right time. When a threat intelligence operations tool incorporates additional insights into how specific feeds are performing, analysts have a better basis for making decisions about which feeds to enable for their individual environment. For instance, the ThreatConnect's CAL provides Intel Report Cards, which enable analysts to tell at a glance how much credibility to give a particular indicator of compromise (IOC), based on what's known about its source.

# Operationalizing Threat Intelligence: The Key Capabilities

To be able to advance the effectiveness of an organization's SecOps program (and its cybersecurity maturity overall), CTI needs to be operationalized, which can be distilled into these four core activities.

### Aggregation

Consolidate data from a diverse variety of sources – external threat feeds, community and information sharing consortiums, and internal sources like incident response reports, and other security tools, which becomes a single source of truth for anyone who needs access to this information. This enables security analysts to pivot (i.e., place information in context by relating it to other threat activities and external intelligence) during an investigation.

### Analysis

CTI should help security teams – from analysts all the way to the CISO – understand which threats are most relevant to their specific role, as well as which pose the greatest risk to the business (see Intelligence Requirements above). Analysis can be manual but should be automated whenever possible because this generates faster, scalable results. High-quality analysis is a critical step that must produce high-quality, high-fidelity threat intelligence before security teams can act upon threat intelligence.

### Action

CTI needs to be actionable, or else it has diminished value and utility. It needs to be provided to the consumers as high-fidelity CTI that can support other processes, like incident response, threat hunting, and vulnerability management. It needs to integrate with detection and defense technologies so that it can be seamlessly incorporated into monitoring and incident response workflows. This dissemination of information is what enables the security program to derive value from the insights it produces.

### Automation

CTI integrated with workflow, task and playbook automation capabilities, can reduce the workload and enable teams to make better security and business decisions. Almost any cyber security task can be automated: examples include performing data enrichment, triaging malware, and blocking threats.

When it's integrated into all aspects of security operations, threat intelligence enables cybersecurity teams to focus on what matters most. **This increases the effectiveness and efficiency of the security team overall, and thus enhances the organization's overall security.**

02

# The ThreatConnect Platform: The Foundation for Threat Intelligence Operations

The ThreatConnect Platform centralizes the aggregation and management of all the threat data that's relevant to your security program within a single platform. Automation enables CTI to be operationalized reducing the overhead required to aggregate, analyze, and action intelligence.

This makes it possible for TI Ops and SOC analysts, incident responders, threat hunters, and business decision-makers alike to have a clear view of the current threat landscape – one that can provide a basis of evidence for human decisions or be used to drive automated response actions.

The Threat Connect Platform **contains a wealth of capabilities** and integrations. For the purposes of operationalizing Threat Intelligence, we will focus on the following:

- **Threat Intel Library:** Lets you automatically and continuously aggregate, correlate, and operationalize intelligence from multiple sources at scale.
  - **Threat Intel Data Model:** Lets you store data as either indicators (such as hosts or URLs) or groups – collections of related behavior and intelligence (such as adversaries or emails). Can be associated with each other, to show patterns in the data.
  - **Threat Intel Scoring:** Lets you prioritize responses by assigning threat ratings to observed indicators. Distills multiple factors down to a single, actionable score based on average threat and confidence rating across all sources.
- **Collective Analytics Layer (CAL™) :** ThreatConnect's innovative analytics engine distills billions of data points, and offers immediate insights into the nature, prevalence, and relevance of a threat. It provides global context from numerous sources and collections, including the community of ThreatConnect users.
- **API:** The ThreatConnect API allows users to programmatically connect different software solutions so they can communicate and facilitate activities. Detect threats, retrieve alerts, perform data enrichment, gain relevant threat intelligence, and conduct incident response actions programmatically.
- **STIX and TAXII Support:** Structured Threat Information Expression (STIX™) is used to facilitate the exchange CTI and Trusted Automated Exchange of Intelligence Information (TAXII™) is an application protocol for securely exchanging CTI.
- **Marketplace:** The Marketplace is a one-stop shop for ThreatConnect Apps that enable easy integrations with 3rd party tools, as well as offering a variety of Playbook Templates.
- **Automated Playbooks:** Automate cybersecurity tasks and processes, and connect hundreds of technology solutions together using a drag-and-drop interface.
- **Workflows:** Increase efficiency and accuracy by allowing security teams to combine manual and automated operations to define consistent and standardized processes for the security team. These might include malware analysis, phishing triage, alert triage, intel requirement development, escalation procedures, and breach standard operating procedures.
- **Threat Graph:** Improve threat intelligence and investigations through visualization with context; understand complex relationships to better understand indicators and tell a meaningful narrative around them.
- **Dashboard, Alerting, Reporting:** Easily visualize data that shows the impact of your security efforts, and gain understanding of emerging threats. Monitor your security operations and intelligence.

# Operationalizing Threat Intelligence

### A Single Source of Truth Encompassing Diverse Data Sources

When you use the ThreatConnect Platform as your TIP, it can manage massive amounts of information from diverse sources. It's able to normalize data, enrich it with additional context, and automate manual threat intelligence-related security processes. This facilitates rapid response and gives all stakeholders a panoramic view of the current threat landscape.

The ThreatConnect Platform can incorporate intelligence from a broad array of relevant sources. The platform, through a number of its capabilities, enables the refinement of data from cases, incident response engagements, threat investigations, defender forums, open-source communities, and vendors. This makes situational awareness and historical context available for use in decision-making. It also makes it possible to share unified intelligence across the business and security team.

### Decrease Ambiguity to Make More Confident Decisions

You can make better decisions that are based on the high-fidelity intelligence that's most relevant to your individual organization. Decisioning will evolve in tandem with changes in the intelligence that's driving the process, thanks to CAL™ that distills billions of data points, offering immediate insights into the nature, prevalence, and relevance of a threat. This process can be automated, to ensure that the very latest intelligence consistently informs all decision-making. And your processes will improve over time, based on new learnings.

### Prioritize Response Actions Based on Threat Severity

ThreatConnect's ThreatAssess intel scoring feature lets your team assign threat ratings to the indicators you observe. It distills multiple factors down to a single, actionable score, based on threat and confidence ratings across multiple sources. Intel ThreatAssess can be combined with CAL™ which produces communitygenerated scores. Included reports explain why an indicator earned a particular score, providing valuable context. Over time, organizations can fine-tune their score to be more accurate and relevant to their organization.

### Understand the Complex Relationships Between Pieces of Threat Intelligence

The ThreatConnect Platform leverages a robust data model (the Threat Intel Data Model) that reveals relationships between threat actors, campaigns, incidents, and IoCs, giving your team deeper insights into relevant context around alerts and incidents. You can build up the Threat Intel Library, and benefit from the Threat Graph capability to get a visual representation of the relevant threats.

### Enhance Intelligence with Global Contexts

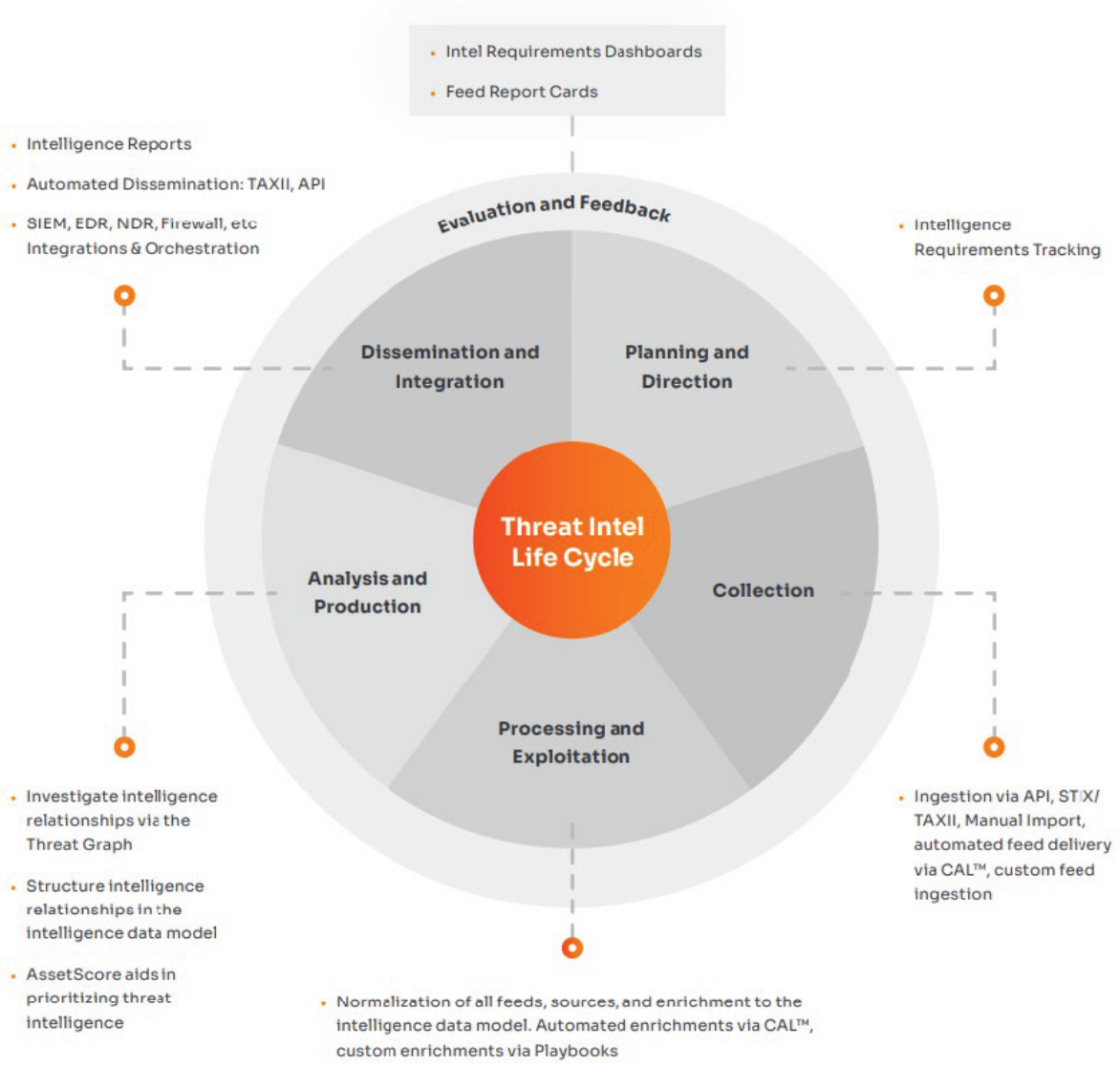
You can leverage data from CAL™ to gain additional insights from thousands of ThreatConnect users around the globe. This gives you more intelligence on threat actors' latest tactics to help you identify malicious activity faster. You can also contribute Artifacts to ThreatConnect's intelligence repository to help other security teams during future investigations.

### Automate nearly any Action and Process

Playbooks enable a range of tasks and processes to be automated, ranging from malware analysis and blocking actions. This ensures consistency across your processes, creates efficiencies, and reduces manual effort seamlessly. The ThreatConnect Platform provides a high-level of interoperability with your existing security tools, allowing you to connect and automate across your tech stack all from a single pane-of-glass.

03

# How ThreatConnect Facilitates the Intelligence Cycle




Support the mission and purpose of a cyber threat intelligence team to inform stakeholders of the threat landscape and lower risk to the organization through enabling a proactive security team.

# The Benefits of Operationalizing Threat

It's no secret that being overwhelmed is par for the course inside cybersecurity teams. And the events of 2020 and 2021 have amplified the stressors and challenges that SecOps professionals confront. In one recent survey, 70% of security professionals said that their home lives were negatively impacted by the threat and alert volumes they faced at work. 54% described themselves as "drowning in alerts" and 55% said that they were simply unable to prioritize and respond to threats at work.[9]

When leveraged to help security teams work smarter not harder, properly operationalized CTI has the power to dramatically improve security teams' on-the-job performance, professional satisfaction, and sense of accomplishment. It can do so by enabling them to direct their efforts where they'll make the biggest difference.

The ThreatConnect Platform capabilities is an enabler for the operationalization of threat intelligence across security operations providing a range of benefits.

**The Advantages of Automation:** The ThreatConnect Platform provides the ability to leverage the Threat Intel Common Data Model, the Threat Intel Library, and Intel Scoring with Playbooks and Workflows, taking advantage of automation to perform routine tasks and activities.

**Linking Cases and Intelligence:** A platform with native automation and orchestration enables every event to be enriched with invaluable contextual information. This makes it easy for analysts and incident responders alike to understand defined as well as probable associations.

**Enhancing Detection and Alert Triage:** Indicators of compromise (IoC) and detection signatures canbe leveraged to enhance detection capabilities across the whole of your cybersecurity solution ecosystem. The ThreatConnect Platform can inform and enrich alerts generated by SIEM platforms along with network detection and response (NDR), endpoint detection and response (EDR), and the rest of your security and IT solutions tools to enhance the entire ecosystem's accuracy and intelligence. This will reduce false-positive rates and speed time-to action by providing insights and relevant context.

**Adding Actionable Artifact Context:** The ThreatConnect Platform includes highly flexible and customizable dashboards that makes it easy to correlate context with artifacts and eventsso that analysts have a deeper understanding of the relationships between potentially malicious activities, making threat intelligence available everywhere.

**Making Threat Intelligence Available Everywhere:** With the ThreatConnect Browser Extension, analysts can instantly scan and identify relevant pieces of information from any web-based resource or web-based security tool. The Browser Extension leverages natural-language processing to analyze and provide novel insights, such as a mapping to MITRE ATT&CK (TM) tactics, techniques, and procedures, and translating threat actor aliases.

9 Phishing activity trends report

04

# Close the Gap Between Knowledge and Action: Leverage the Power of the ThreatConnect Platform

There's a dramatic difference between security tools and solutions that simply ingest threat intelligence and those that are smart and flexible enough to make it actionable. This refined intelligence enables analysts and incident responders to automate routine actions or make better decisions during event triage, investigation, and remediation.

## Security Monitoring and Alert Triage

High false-positive alert volumes remain one of the greatest challenges that SOC analysts face. When threat intelligence is used to provide contextual enrichment of alerts and events, it enables analysts to "connect the dots" with greater confidence. If a SIEM solution is ingesting invalidated, raw threat feeds, it's going to result in excess of noise – along with unnecessary triage and overwhelmed, unproductive security teams. Threat intelligence operationalized with the ThreatConnect Platform aggregates and rationalizes the threat data the SIEM receives. This transforms noise into a clear signal that improves alerting accuracy and makes it easier for analysts to spot trends or patterns that are out of the ordinary.

## Phishing

Phishing is an old and well-established cyber threat that still tops the list of the most popular initial attack vectors. And phishing activity reached new heights during the pandemic. According to the AntiPhishing Working Group, January 2021 saw the highest-ever monthly total of phishing attempts in the group's reporting history. Then the record was broken again in July 2021, with an unprecedented 260,642 phishing attacks.[10]

10 Phishing activity trends report

Having accurate phishing threat intelligence on hand makes it possible for security teams to quarantine known phishing emails before they ever reach employees' inboxes. When this intelligence comes in a form that's readily integrated with email security solutions and other network protection products, security teams can act with speed and confidence, or automate response actions to known phishing threats. Furthermore, should a phishing attack be successful, orchestration and automation capabilities will provide a workflow that enables rapid and successful successful response and containment of the incident.

A subset of phishing attempts, Business Email Compromise (BEC) attacks have become more prevalent over the past year. One recent study found that 71% of organizations had experienced a BEC attack between 2020 and 2021, with the majority of these attacks leveraging spoofed identities, look-alike domains, or compromised account credentials.[11] Such attacks are notoriously difficult to detect, especially at scale. SecOps teams often need to review emails manually to identify fraudulent communications. With accurate, current threat intelligence, they'll know exactly where to look, saving time and effort while improving detection accuracy.

## Incident Response and Threat Hunting

Having accurate information about the capabilities of threat actors enables security teams to understand their strategies as well as their TTPs. Responders can use threat intelligence to accelerate investigations since this information provides essential context and direction that can help them piece together cause and effect, and understand the relationships within event chains. Threat hunters often begin hypothesis-based hunts with a particular piece of threat intelligence in mind, searching for evidence that current threat actors have been present in the environment.

11 2021 Business Email Compromise Report

# Conclusion

**Smarter Security, Maximum Impact**

Today's cybersecurity professionals face a myriad of challenges, including tireless, resourceful, and endlessly innovative adversaries. But informational asymmetry no longer needs to be among the stumbling blocks that hold defenders back. A TI Ops team with the best tool can help right the balance of power between attackers and defenders. The ThreatConnect Platform is your security team's secret weapon against attackers. It allows TI Ops and SecOps teams to move beyond just managing threat intel, to operationalizing it for maximum impact, and to optimize their insights, efficiency, and collaboration.

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. now a part of Dataminr.

ThreatConnect enables security operations and threat intelligence teams to work together for more efficient, effective, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse threat intelligence and cyber risk quantification into their work, allowing them to orchestrate and automate processes to respond faster and more confidently than ever before. Nearly 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their most critical systems. Learn more at **www.threatconnect.com**.

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