
A Disconnect in Threat Intelligence
IS IT TIME FOR A MORE
STRATEGIC APPROACH?
CENTRIPETAL

Introduction:

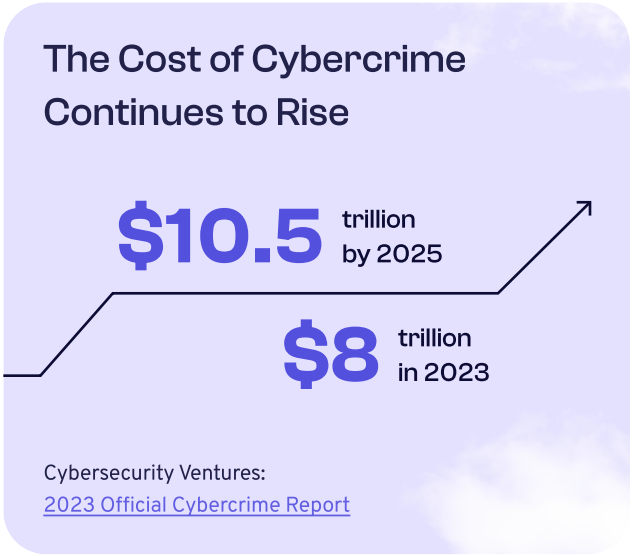
Rising Cybersecurity Threats Demand a Bold New Approach

The fast pace of digital transformation fuels business growth around the world – but unfortunately, it also heightens exposure to cybersecurity threats. Exposure to these threats due to increased vulnerabilities can quickly turn into breaches with devastating economic impact: the global cost of cybercrime today is $8 trillion, and it's estimated to hit $10.5 trillion by 2025.

Whether it's malware, phishing, ransomware or DDoS attacks, cyberattacks are increasingly difficult for organizations to avoid, with 47% of U.S. businesses experiencing some form of cyberattack in 2022. And, sophistication is scaling quickly with attackers deploying innovative methods to bypass standard security measures, such as AI-powered intrusions and last-minute domain changes. Adding to this, the widespread availability of pre-built hacking tools and the increased availability of access broker services has lowered the barrier to entry for new hackers.

In the face of escalating cyberwarfare, high confidence threat intelligence (TI) and effective analysis is an integral part of any cybersecurity strategy. Consequently, organizations are procuring more data sources, including TI feeds, and hiring skilled analysts to make sense of it all. 63% of cybersecurity professionals say they're spending significantly more money than ever before on cyber threat intelligence (CTI) programs.

Despite this abundance of effort, they're still struggling to make data-backed decisions – 79% say that majority of the time, they make decisions without adversary insights. Because of this, cybersecurity teams are reacting after threats have already happened, and failing to achieve the desired impact from their TI investments. That's why 71% say they have difficulty measuring any ROI or benefits of their CTI programs.



In order to see the full promise of TI, security teams must adopt a more proactive approach:

At Centripetal, we call this Adaptive, Real-Time Threat Intelligence (ART), which requires comprehensive TI coverage, rapid detection and skilled analysis – designed to prevent a greater number of breaches before they occur.

This paper will explore why the traditional approach isn't working against today's threats and how ART Threat Intelligence can help organizations detect and mitigate threats earlier, reducing the burden downstream and strengthening security across the enterprise.

CURRENT THREAT INTELLIGENCE PROGRAMS MISS THE MARK

Today's security teams are in a perpetual state of reaction, retroactively reviewing breaches and adjusting security policies to prevent the next attack. This may have been a sustainable approach when both organizations and the hackers themselves were limited by lack of advanced tools and technologies.

But now, hackers have adopted increasingly sophisticated techniques, and organizations have yet to adapt their technologies and processes to handle these new threats – creating a mismatched playing field that puts organizations at a disadvantage.

While recent developments in CTI programs showed promise in better supporting organizations, it has become apparent over time that CTI programs still lack the structure,process, and objectives to realize value. They're simply unable to keep up as threats evolve, presenting significant challenges that elevate the risk of security incidents.

> **"Today's global cyberthreat landscape is constantly evolving and becoming more sophisticated, requiring a more proactive and adaptable approach to cybersecurity.**
>
> **Collectively, we have the power and the responsibility to build a secure digital world, and it begins with neutralizing the ever-present and constantly evolving cyberthreats."**
>
> Jonathan Rogers, Centripetal COO

Challenge 1

Limited TI Feeds Don't Offer Enough Protection

Your TI vendors may claim to have unique intel – and it's possible they do. But without a high volume of feeds, you may not see the right indicators of compromise (IOCs) to truly understand the threat. **There's at most a 4% overlap between different TI feeds, revealing significant gaps in coverage.** This leaves organizations in the dark, seeing 0.1% of the IOCs crucial for detecting threats effectively.

Challenge 2

The Current Methodology is Too Slow To Prevent Attacks

On average, it takes an alarming 207 days to detect a breach and an additional 77 days to rectify the damage. This sluggish response is rooted in the highly manual process required to scrutinize the abundance of data and sort through millions of events recorded in security information and event management (SIEM) systems.

Minor security events can quickly evolve into higher-risk threats, so while teams are reacting, the threat is already occurring. For a truly effective security posture, teams must have the tools and information at their fingertips to detect attacks in real-time and quickly launch an effective response.

Challenge 3

Existing Tools and Technologies are not Designed to Process a High Volume of IOCS

While some networking products leverage TI to detect or block threats, traditional tools can't do this at the levels needed. They may struggle to filter out the "noise" within network traffic, hindering their efforts to detect the real threats.

Consider your current system's limitations: your firewall can likely manage 50,000 to 150,000 rules, based on the product. These rules are fixed and need to be managed manually. But, there are many potential threats in the world at any given time, meaning your firewall covers only a tiny fraction of all known threats. Without real-time threat updates or context, your team is overloaded with log data, missing event data on the majority of your network traffic.

Without major computing power and automation to detect patterns of concern, the volume of modern cyberattacks simply exceeds the capacity of most organizations. It doesn't have to be this way: 95% of breaches could have been prevented with the right technology in place.

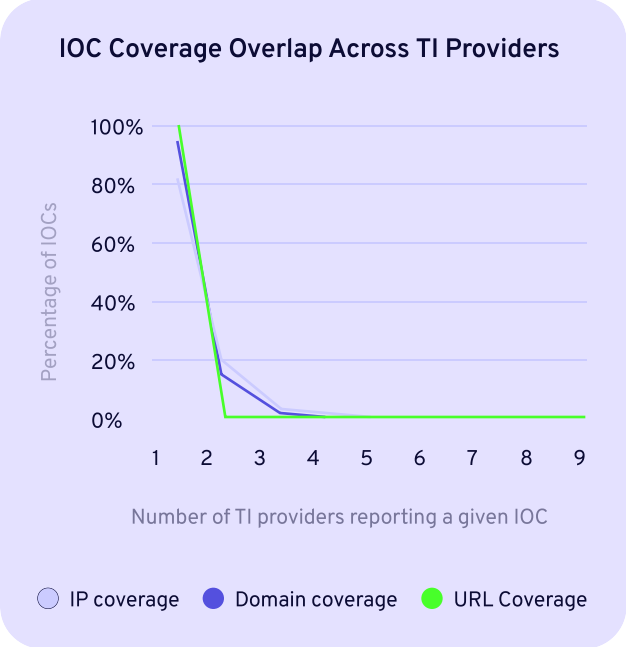


Figure 1: IOC coverage overlap measured across TI feed providers. High percentage of IOCs are only reported by a single TI provider, indicating no overlap and thus insufficient coverage with a few TI feeds.

ESG Technical Validation: CleanINTERNET by Centripetal, 2022

SECURITY TEAMS STRUGGLE TO KEEP UP, REQUIRING A MORE DYNAMIC SOLUTION

Both team size and skillset are a hurdle for security teams working to protect their organizations: 63% of cybersecurity professionals say that they don't have the necessary staffing or skills in-house to effectively run a program for their organization. Another 60% of businesses report they have trouble holding onto qualified cybersecurity staff.

Security teams are falling behind.

63%

of cybersecurity professionals say that they don't have the necessary staffing or skills in-house to effectively run a program for their organization.

ESG: Cyber Threat Intelligence Report, 2023

Small companies often have limited security or IT teams, and even enterprises, despite having dedicated analysts, struggle with the sheer scale of security events. For instance, organizations frequently witness tens of millions of security events per day across various devices including firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), Deep Packet Inspection (DPI) systems, and web filters. This load only escalates as the security industry generates even more events with newer approaches emphasizing observability and telemetry for detection and response.

Applying security rules based on threat data across a variety of devices adds to the team's burden and leads to delays. These devices, typically managing only a few hundred thousand rules, can also experience performance issues when tasked with extensive rule-based packet filtering. Additionally, the use of TI for forensic analysis in Security Information and Event Management (SIEM) systems poses similar challenges.

These conditions compound the pressure on security teams. Ultimately, despite considerable investments in security, organizations remain exposed as the risk of compromise escalates, highlighting the need for a more comprehensive, robust, and automated threat management strategy.

ADAPTIVE, REAL-TIME THREAT INTELLIGENCE ADDRESSES THE MODERN THREAT LANDSCAPE

A new approach to cybersecurity, one that can effectively scale with the volume, speed, and changing nature of threats is possible with the right tools in place. ART threat intelligence proactively blocks breaches, improving response times and preventing future attacks. Teams must put several strategies in place to leverage this new approach.

Strategy 1

Increase Your Intelligence Coverage

A handful of TI feeds will not be enough to protect your organization from today's sophisticated threats. To get a comprehensive, real-time view of threats, enterprises should increase the number of high-quality TI sources and feeds. But that can be cost-prohibitive, particularly for smaller organizations.

Instead, look for tools that aggregate information across many TI providers, consolidating many sources of intelligence into a single, curated feed. These tools can significantly broaden your awareness of threats, help you identify emerging threats, track the activity of known threat actors, and better assess the risk of being targeted.

Strategy 2

Automate the TI Pipeline From End to End

Speed is one of the most critical characteristics of a proactive defense. When a new IOC or threat source is identified, you'll want to block malicious traffic as soon as possible. Automated TI tools quickly process large volumes of data, identify highest-risk threats, and allow you to incorporate information into your security infrastructure within minutes – matching the speed at which attacks can break out.

Look for TI tools that seamlessly integrate intelligence with existing technology in actionable ways – automation has to be embedded in the entire process to be most effective. Furthermore, focus on tools that update the TI pipeline in near real-time, within minutes, given the speed at which compromises can turn into breaches and crossover to adjacent systems.

Strategy 3

Reduce Noise for Timely Accurate Intelligence

Security teams operate best when receiving high-quality, accurate, and timely threat intelligence. However, traditional security measures such as firewalls and router ACLs struggle to filter the noise of network traffic. Events, alerts, and logs of security technologies such as IDS, Extended Detection and Response (XDR) and Network Detection and Response (NDR) add to the cacophony, making it difficult for security analysts to find the serious, credible threats – akin to searching for a needle in a haystack. But instead of searching faster for the needle, reduce the size of the haystack.

Utilize powerful packet filtering services to block more known threats before they reach your security team. Look for ones that can operate at line speed and even protect you in the cloud.

Strategy 4

Uplevel your Threat Analysis Capabilities

Your last line of defense is your security team's vigilant analysis of threats that remain. But not all organizations are applying the time and resources required on this analysis phase, and security teams report cyberthreat analysis as their least proficient area in the CTI lifecycle. The obvious answer might be to hire and train more qualified analysts, but there are better options.

Security operations (SecOps) services can augment your in-house security teams with dedicated security analysts. This is not about hiring contractors instead of full-time employees. This is about upleveling your threat analysis capabilities with highly trained analysts who have greater visibility of the threat landscape across your industry or the globe.

Also, AI-based threat detection can now help human analysts improve response times as well as identify more patterns and threats before they become a breach. Look for tools that incorporate AI and machine learning to pull out the highest quality intel from multiple incoming and outgoing streams, thus focusing your security team's attention on the most credible threats.

Conclusion:

IT'S TIME TO EMBRACE ADAPTIVE, REAL-TIME THREAT INTELLIGENCE

Threat Intelligence in Action

Challenge:

A large northeastern health system was struggling with 6M firewall events per hour (up to 63M daily), driving up storage costs in its SIEM system.

Solution:

Implementing Centripetal's CleanINTERNET® , the system dramatically reduced firewall events, experiencing only 500K per day, a 120x reduction. They also went from storing 5.7GB to 11.7MB per hour, leading to considerable cost savings. After two months and a few rounds of high confidence threat shielding, there were zero disruptions to the network.

"We've gone from 3M blocks an hour to 20,000 an hour, to 6,000 an hour. What we will now record in SIEM from outside-in blocks over three weeks is what we used to record inSEIM in one hour."

Senior Cybersecurity Architect, Large Northeastern Health System

Traditional methods are unable to manage the ever-evolving threat landscape. The increasingly contentious battle against cyberthreats demands a dynamic, forward-thinking approach, one that leverages advanced threat intelligence to proactively protect organizations.

It's time to broaden your intelligence coverage, fast-track response with automation, cut through the noise, and fuse human and AI-powered analysis. By doing so, you're not just refining your defenses, but revolutionizing them. Let's step into this new era, prepared, vigilant, and stronger than ever.

ABOUT CENTRIPETAL

Centripetal, a global leader in intelligence powered cybersecurity, is operationalizing the world's largest collection of threat intelligence, in real-time, to protect organizations from every known cyberthreat through its innovative patented technologies. Through its CleanINTERNET® service, Centripetal delivers a highly effective solution leveraging the latest computing technology and skilled operations intelligence analysts at a significantly lower cost.

Powered by the combined threat intelligence of more than 250 of the world's best intel providers, Centripetal incorporates the fastest packet filtering technology on the planet and ensures comprehensive protection against the latest cyberthreats based on real-time threat intel. Centripetal's CleanINTERNET® reviews more than 3,500 cyberthreat feeds every 15 minutes to shield against 99% of known threats.

Centripetal's elite team of highly trained intelligence operations analysts acts as an extension of its customer's internal cybersecurity team, who monitor and analyze emerging threats. This mitigates the skills gap and reduces the burden on overworked IT resources.

Ready to Take the Next Step?

For more information about how Centripetal's sophisticated approach to threat intelligence can protect your organization, please

CONTACT OUR SALES TEAM ↗


CENTRIPETAL