White Paper

Centripetal Networks Threat Intelligence Gateway

Designed to Enable Continuous Prevention Through Intelligence-led Enforcement

By Tony Palmer, ESG Senior IT Validation Analyst

May 2018

This ESG White Paper was commissioned by Centripetal Networks and is distributed under license from ESG.

Contents

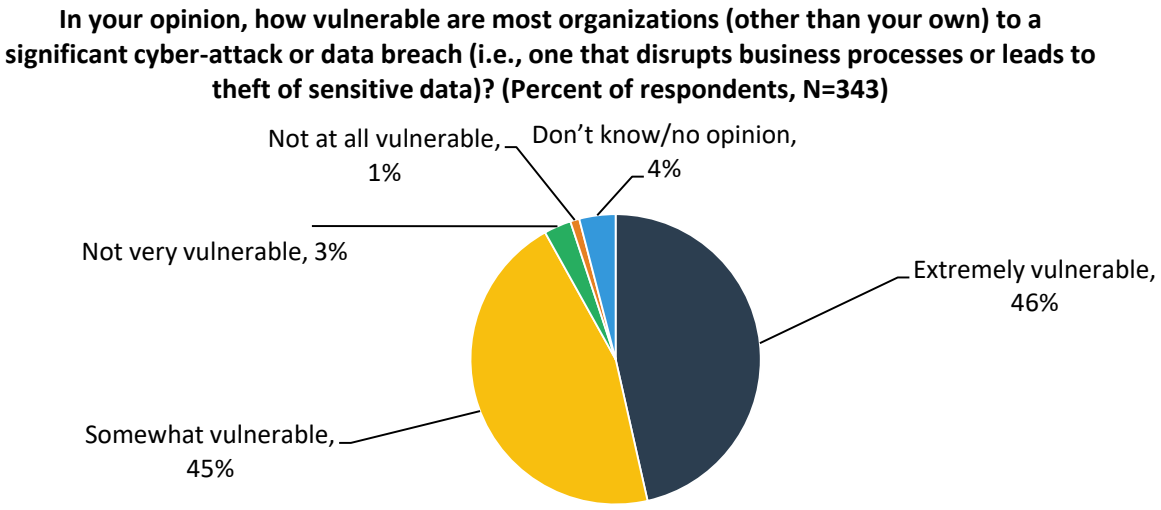
Abstract

The promise of cyber threat intelligence (CTI) for cyber-defense has been talked about for years. In response, many enterprises have tried to integrate feeds into their security operations centers (SOCs), have purchased new threat detection technologies, and have created custom intelligence programs to counter threats. ESG research reveals that a vast majority of midmarket and large enterprises have some type of CTI in place, but 39% of respondents report that manual processes and individuals are still used to aggregate and analyze the intelligence collected.[1] When intelligence is used only for forensics as a manual, post event process, many cyber-attacks go undetected for weeks or months as exposure and damages escalate over time. Manual processes don't scale well and the forensic focus on security emergencies can cause enterprises to miss out on the benefits of proactive, preventive intelligence-based defense. In addition, many firms lack the right level of skills and experience with CTI. To improve CTI program effectiveness and ROI, CISOs need solutions designed for intelligence that normalize sources by risk, shield the environment, and triage known threats in real time, in line with the network at full network speed while providing for visualization and workflow.

Overview

Organizations large and small face a difficult situation in today's threat landscape. More adversaries are employing more exploits to deliver more malware with increasing sophistication. The volume of security events is far too high to process manually, and firms simply can't keep up with the deluge of evolving threats—both known and unknown—leaving them vulnerable to breach. This is reflected in a research project from ESG and the Information Systems Security Association (ISSA). Alarmingly, 91% of surveyed organizations claim that they are significantly vulnerable or somewhat vulnerable to a cyber-attack or data breach that will disrupt business processes or steal data (see Figure 1).[2]

Figure 1. Vulnerability of Most Organizations to Cyber-attacks and Data Breaches



Source: Enterprise Strategy Group

Threat Intelligence

[1] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.
[2] Source: ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals*, November 2017.

Most CISOs recognize that they are ill-prepared for today's threat landscape and are investing in new cybersecurity staff, processes, and technologies to help bridge this gap. In fact, ESG research revealed that 69% of organizations planned to increase their cybersecurity spending in 2017.[3]

Threat intelligence represents the work-product of security experts globally. This data provides significant benefit to an enterprise that cannot duplicate similar expertise internally. This is the promise of threat intelligence. As a result, threat intelligence programs are a segment of cybersecurity that organizations are actively targeting for improvement. Many firms are gathering more threat intelligence data. ESG research reveals that 28% of organizations collect, process, and analyze substantially more security data than they did two years ago.[4] Aside from internal security data, many firms have increased consumption and analysis of external open source and commercial threat intelligence feeds. In the past, threat intelligence was often collected and analyzed by a wide assortment of compliance, security, and IT personnel. This led to tremendous inefficiencies with various threat data spread haphazardly across organizations. To alleviate this problem, CISOs are building central services for threat intelligence collection and processes.

Threat Intelligence Challenges

The end goal of a threat intelligence program is defense in advance of an event. Intelligence provides a risk-based awareness of network threats to prevent known threats and to empower organizations to act upon high risk events faster. Unfortunately, ESG has found that multiple challenges stand in the way of operationalizing threat intelligence in a high performance, and high-fidelity way. These factors cause many threat management programs to miss out on the promise of threat intelligence:

- Lack of automation. According to ESG research, 39% of organizations rely on manual processes to aggregate and analyze raw threat intelligence today.[5] This means that they rely on humans to collect, analyze, contextualize, and enrich CTI—before they can extract any benefit. The volume and dynamic nature of the data make this an impossible task for the workforce within any individual enterprise to stay current. This prevents organizations from getting and understanding the intelligence in time to do anything about it.

- Forensic posture. Many organizations consume open source and premium feeds using multiple products. They often share data with industry Information Sharing and Analysis Centers (ISACs) and purchase custom reports and services for monitoring impending threats. Unfortunately, this data is almost never applied in a meaningful way to live network traffic and even less frequently applied inline for a protective benefit. As a result, the intelligence process which in general is intended to inform a decision in advance of an event is at best used to provide context after an event. The technical challenges with moving intelligence to a pre-event posture are extremely difficult with legacy network enforcement tools. Security teams must develop the ability to organize, analyze, and act on this information in advance of the risk event.

- CTI risk-based workflow. Threat Intelligence is spread across a risk spectrum. This is a new and difficult concept for enterprise security teams. Traditional network security enforcement operated on a binary "yes" or "no" use basis, but today's intelligence enforcement decisions are about managing risk across a continuous spectrum. Organizations must develop the ability to rapidly triage based on risk and to collect all the relevant data needed by human analysts. The bandwidth of the human analyst must be carefully preserved. Managing the overwhelming volume of CTI data through manual processes wastes valuable time and effort, causing organizations to struggle turning CTI into actionable insight, i.e., knowledge that can be used to fine-tune security controls, generate remediation rules, or

[3] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.
[4] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.
[5] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.

communicate risk to business executives. This also directly affects their ability to take timely action on a given piece of intel.

CISOs see the promise of threat intelligence and continue to spend on threat intelligence programs even while getting a generally poor return on their investment.

Threat Intelligence Gateways

It seems like there should be a solution to these challenges. When threat intelligence points to bad IP addresses, URLs, or DNS lookups, why not simply block them? This has been more difficult than it sounds, as it involves normalizing disparate threat intelligence feeds, building custom rule sets, integrating network security devices, and operationalizing all of it. The technology challenges here are significant. Threat intelligence gateways are designed to alleviate the data management, policy management, and performance challenges described above with purpose-built network enforcement points that:

- Normalize threat intelligence. Threat intelligence gateways are designed to consume and normalize threat intelligence directly, obviating the need to parse cryptic threat intelligence feeds or integrate various types of threat intelligence and security analytics with existing network security infrastructure.
- Provide policy management. Rather than rely on custom analysis and manually built rule sets, threat intelligence gateways provide policy management dashboards and tools that provide security teams the ability to easily configure rule sets to block known threats based upon risk, threat sources, or other complex criteria. This enables threat intelligence gateways to allow a CISO to create company-specific policies for blocking industry-focused attacks, targeted attacks, and more generic "noise" from threat actors.
- Operationalize threat intelligence. Threat intelligence gateways aren't "set-it-and-forget-it" solutions, but they can be extremely efficient in helping organizations streamline security operations and massively cut event volume, while mitigating risk. They do this without requiring a one-off integration or customized code.

Threat intelligence gateways typically live between an edge router and a firewall and can start to deliver value right after deployment. In this model, threat intelligence gateways filter traffic and reduce security event load.

Many next-generation firewall vendors like Cisco, Check Point, Fortinet, Juniper, and Palo Alto Networks offer traffic filtering based upon threat intelligence today, which begs the question: Why not just do this with a next-generation firewall and eliminate the need for another system?

While next-gen firewalls can filter traffic based upon threat intelligence, this process consumes resources and processor cycles, which can impact firewall performance. Threat intelligence gateways are purpose-built and designed for complex, highly dynamic policy management for threat intelligence-based rules. Alternatively, next-gen firewalls are built for a wide assortment of application, network, threat, and user-centric rules designed around static acceptable use models. Threat intelligence network rules change by the minute, massively exceed the scale of firewalls, and require more granularity than is possible in a traditional enforcement point.

Threat intelligence gateways aren't for everyone, but large organizations with massive global networks have a large target on their backs and need all the help they can get. For these enterprises, threat intelligence gateways may provide strong benefits for a relatively little cost.

Threat Intelligence Defense: What's Needed?

To transform today's threat intelligence chaos into a more efficient, effective, and useful resource, security teams must move forward with a threat intelligence strategy that includes the following:

- The ability to consume and process the growing range of CTI data. Threat intelligence information will continue to grow based upon new technology targets and cyber-adversary tactics, techniques, and procedures (TTPs). Therefore, threat intelligence programs should be able to leverage a wide variety of threat intelligence, including open source intelligence (OSINT) like blogs, social media, etc., commercial threat feeds, industry feeds from ISACs and ad-hoc industry groups, dark web data, reports, custom feeds, internal intelligence, etc. For organizations to be able to leverage external expertise, an open intelligence architecture is essential.

- A central management and analysis portal. Given the volume of CTI information, security teams need help from technology to correlate, contextualize, enrich, and normalize large volumes of CTI data as efficiently and quickly as possible. This job demands a threat intelligence platform (TIP). The best TIPs will provide a common view of CTI for multiple use cases and users, including security analysts, threat hunters, incident responders, vulnerability managers, GRC personnel, risk managers, etc.

- Customization options. Threats come in many shapes and sizes, attacking different organizations in different industries. Additionally, users like security analysts, threat hunters, and compliance professionals use threat intelligence in different ways to get their jobs done. Given this diversity, security leaders should make sure that their threat intelligence platform is highly customizable. This demands the ability to create specific dashboards or enhance threat intelligence with tailored internal notes, white lists/black lists, risk scores, etc., that provide added value on top of analytics. In general, TIPs should be able to filter, sort, query, share, and add custom notes to threat intelligence for all users and use cases.

- Advanced analytics. As previously stated, ESG research indicates that security analysts find it difficult to keep up with threats or manage the volume of security alerts generated by threat detection tools. Threat intelligence solutions should help organizations alleviate some of that pain through advanced analytics. Machine learning algorithms can be applied to threat intelligence to determine the types of threats most often seen attacking specific industries like financial services, retail, health care, government, energy, etc. Leading threat intelligence tools will also apply artificial intelligence to predictive analytics to envisage the indicators of compromise (IoCs) and TTPs that may be used for future attacks. In these ways, advanced analytics can act as a "helper app" guiding organizations to apply resources to high priority risks and accelerate investigations and remediation.

- Technology integration. Threat intelligence solutions should integrate with technologies like SIEM, IR platforms, ticketing systems, and security infrastructure that can act as additional sources of local enterprise-specific intelligence. This enables interoperability between threat intelligence tools and a range of security technologies, creating a security operations and analytics platform architecture (SOAPA). According to ESG research, 21% of enterprise organizations have made security operations technology integration one of their highest priorities.[6] Leading CTI technologies should be designed to support these enterprise SOAPA efforts.

- Support services. Threat intelligence analysis can demand advanced skills that may be beyond what many organizations have at their disposal. Since it will be difficult to hire or train security analysts, CISOs will want to work with threat intelligence technology vendors that can help them fill some of their skills gaps. Examples of these services include setting up a threat intelligence program, monitoring deep/dark web activities, creating customized

[6] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.

threat reports, or providing managed and/or professional services for threat hunting. The promise of threat intelligence is an environment where expert providers working across a set of enterprise customers can substantially augment the threat intelligence defense programs within those enterprises.

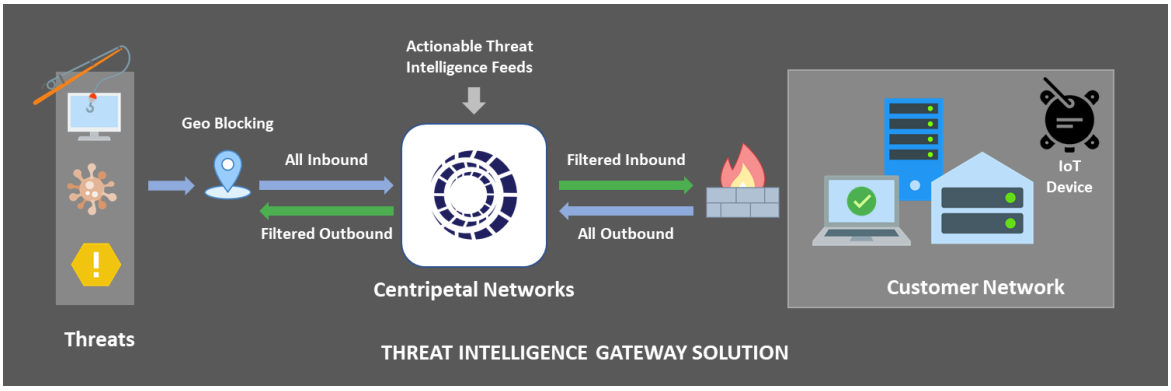
Enter Centripetal Networks

Organizations have been led to believe that they can get what a threat intelligence gateway does from a firewall. The stark reality is that the volume and specialization of threat intelligence calls for specialized tools that can synthesize, analyze, and distribute CTI in real time.

Centripetal Networks' CleanINTERNET intelligence-led managed security service using their RuleGATE enforcement point provides customized threat intelligence filtering designed to significantly reduce security event volume and workload in the enterprise. Centripetal shields the network and dynamically monitors for advanced threats using intelligence. Centripetal's goal is nothing less than the transformation of CTI into protective action at scale. Centripetal does this by converting indicators to rules that drive actions across a risk spectrum, i.e., logging, content capture, mirroring, redirection, shielding, and advanced threat detection.

Minimizing the event workload on analysts increases their efficiency, and enables performance optimization of downstream tools, which can reduce infrastructure costs—fewer intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, sandboxes, anti-malware appliances, packet capture resources, etc.

Centripetal's Threat Intelligence Gateway sits on the wire in front of the firewall and bridges the intelligence gap between the WAN and the enterprise. Organizations considering using their next-gen firewall for threat intelligence-based filtering should seriously consider the distinction between indicators and rules. Vendors that focus on IOC capacity without acknowledging the required network filtering rules can't provide proactive, preventive, intelligence-based defense. CleanINTERNET is designed to enable organizations to move beyond blacklists based on IoCs and better manage traffic by leveraging CTI context with highly granular rules in the form of policies that can be automatically enforced.



Simply put, Centripetal delivers more than is possible with firewalls and IPS systems, which aren't designed for—nor effective at—processing hundreds of millions of indicators from thousands of feeds. ESG watched as Centripetal Networks' Threat Intelligence Gateway solution processed over 140 Gbps of network traffic at wire speed; distributing, ingesting, synthesizing into a network policy, and enforcing over five million complex network filtering rules. Each complex filtering rule contained at-least a dozen unique fields which had to be evaluated and applied bi-directionally and without state. With intelligence enforcement there can be no presumption of insider trust so traditional filters' state assumptions are invalid. The intelligence was dynamically updated without loss and the results were reported in real time for live analytics.

The decision rate observed with this much intelligence and this much traffic is in the range of a quintillion (10^{18}) decisions per second.[7] This is the highest performance network filter that ESG has tested or seen in action to date.

ESG validated that Centripetal Networks' CleanINTERNET managed security service normalizes third-party threat intelligence feeds, blocks alerts and known threats in real time, in line with the network, and provides visualization and process management. Additionally, Centripetal provides implementation, configuration, management, and ongoing threat analysis services with live analyst support for triage, response, and informed threat hunting. An organization's live analysts' workflows are accelerated by Centripetal's AI-Analyst technology, an artificially intelligent machine analyst that focuses the human analysts on the most serious threats.

The Bigger Truth

Threat intelligence has been marketed aggressively and many organizations have increased CTI investment only to be disappointed with the results as they still struggle to operationalize—and benefit from—threat intelligence. The promise of threat intelligence is being able to act in advance of an event, but almost all organizations still cannot do this.

It's time that CISOs recognize that the real value of threat intelligence doesn't come from the data—it comes from the ability to act upon it with efficacy and efficiency. Those organizations lacking the resources and skills to move forward must come to terms with their limitations and find partners like Centripetal who can help them make their CTI programs more productive in short order. CISOs looking for a way to effectively leverage the incredible resource that is CTI would be wise to call Centripetal Networks and see how the company can help.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.