Solution Showcase

Operationalizing Threat Intelligence With a Complete Solution

Date: January 2018 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: Over the past few years, many enterprise organizations have built security operations centers (SOCs), purchased new threat detection technologies, and created cyber threat intelligence (CTI) programs to counter dangerous cyber-threats. According to ESG research, 58% of organizations have had a CTI program in place for at least two years[1] but many firms still struggle to operationalize threat intelligence in an efficient manner. Problems are often due to the fact that CTI programs are built on top of point tools and manual processes. To improve CTI program operations and ROI, CISOs need new threat intelligence technologies that collect volumes of CTI data, centralize data management, include advanced analytics, allow for customization, and integrate with other security technologies.

Overview

According to ESG research, 72% of cybersecurity professionals surveyed say that security analytics and operations is more difficult today than it was two years ago. Why? Cybersecurity professionals point to things like:

- The dangerous threat landscape. Cybersecurity professionals realize that they face determined and dogged adversaries using sophisticated exploits, malware, and social engineering tactics as part of cyber-attacks. Many organizations find it difficult to keep up with the avalanche of constantly changing and persistent threats.
- The growing volume of security alerts. Over the past several years, many organizations added new types of threat detection technologies to their networks, and each tool is designed to sound an alarm when it sees anomalous or suspicious behavior. In combination, these tools can create a cacophony of security alerts. Security analysts are then forced to review, prioritize, and investigate these alerts on their own. While security analysts do their best to keep up, human beings are no match for this type of scale and tend to ignore alerts, chase false positives, and make mistakes.
- The cybersecurity skills shortage. Recent ESG research indicates that 51% of organizations claim to have a "problematic shortage" of cybersecurity skills.[2] This often means they are short-staffed when it comes to skills in critical areas like security analysis, investigations, and threat hunting.

Recognizing these problems, 82% of organizations plan to increase spending for security analytics and operations.

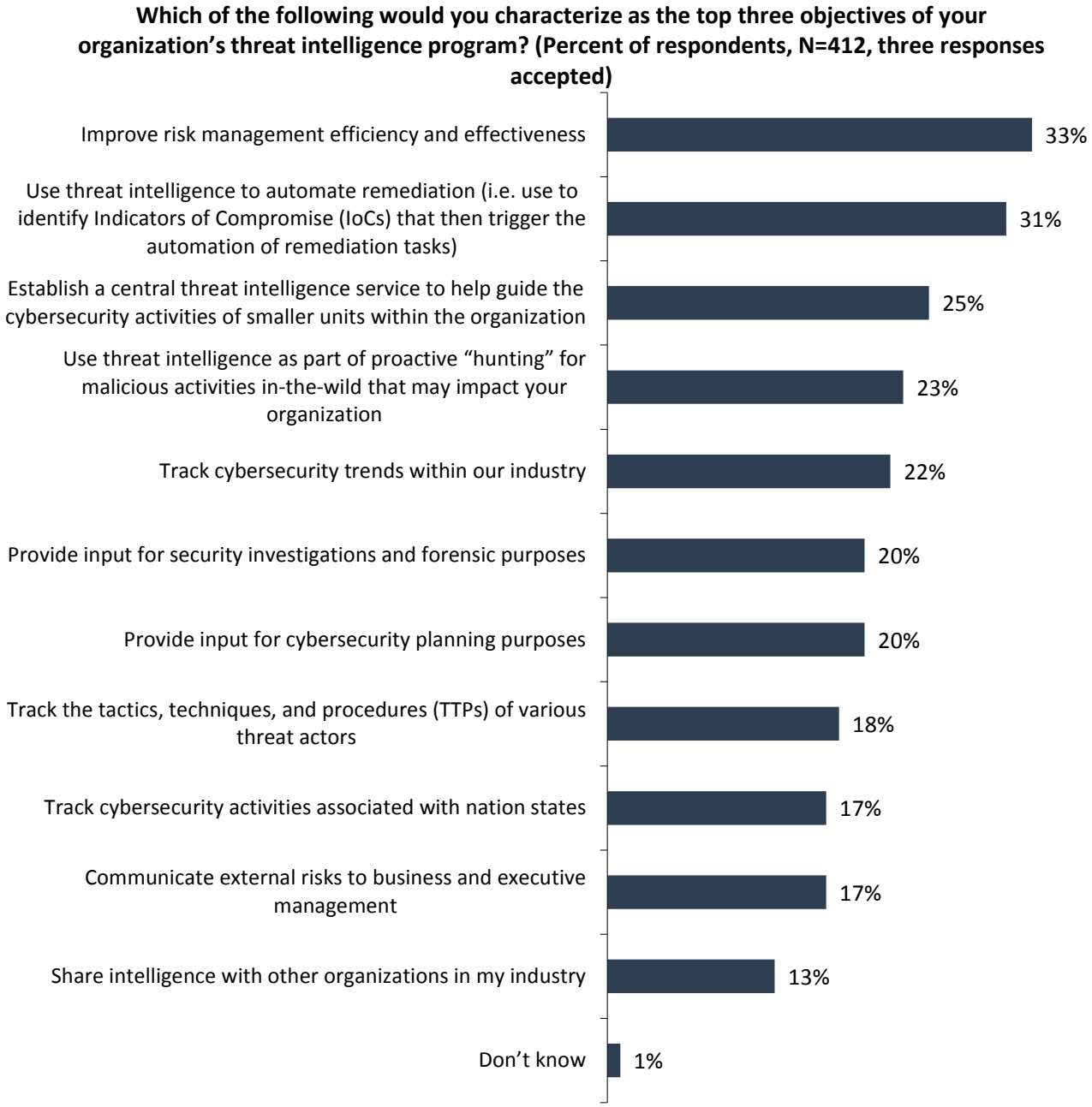
[1] Source: ESG Research Report, *Cybersecurity Operations and Analytics in Transition*, July 2017. All ESG research references and charts in this solution showcase have been taken from this research report, unless otherwise noted.

[2] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Threat Intelligence to the Rescue?

CISOs are always looking for security technologies that can help improve their ability to detect and respond to threats in real time. As part of this strategy, many organizations are purchasing threat intelligence feeds and building threat intelligence programs. ESG research indicates that organizations have numerous objectives for these threat intelligence programs, the most common being improving risk management efficiency and effectiveness, automating remediation tasks, and establishing a central threat management service for the IT and cybersecurity organizations (see Figure 1).

Figure 1. Threat Intelligence Program Objectives



Source: Enterprise Strategy Group

Threat Intelligence Chaos

Threat intelligence program goals are simple: Organizations want to better understand the threat landscape and act upon cyber threat intelligence (CTI) in a timely fashion to reduce risk or respond to incidents. Unfortunately, ESG finds that many threat management programs remain disorganized and inefficient, making it difficult to operationalize threat intelligence in a systematic way. This chaotic situation is driven by:

- **Too many tools and services.** As part of their cyber threat intelligence programs, many organizations consume open source CTI, purchase feeds, view product portals, share information with industry ISACs, and purchase custom reports/services for monitoring impending threats. Somehow, the security teams have to organize, analyze, and gain knowledge from this morass of information.

- **Manual processes.** According to ESG research, 39% of organizations rely on manual processes to aggregate and analyze threat intelligence today. This means that they rely on human intelligence to collect, correlate, contextualize, and enrich CTI—before they can use it for their benefit. This doesn't scale—and has nothing to do with understanding and responding to threats in a timely manner.

- **A struggle to turn CTI into action.** With so much time spent on managing technology through manual processes, organizations struggle to turn CTI into insight that can be used to fine-tune security controls, generate remediation rules, or communicate risk to business executives. This also extends to customizing generic CTI into risk metrics and actions that can be used for a specific organization.

CISOs see the potential benefits of threat intelligence and continue to spend on threat intelligence programs. Regrettably, they also get a very poor return on this investment in return. CISOs must address this unacceptable situation.

Threat Intelligence: 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 featuring (see Table 1):

- **A growing assortment of CTI data.** Threat intelligence information will continue to grow based upon new technology targets and cyber-adversary tactics, techniques, and procedures (TTPs). Therefore, CTI programs should include 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. Leading CTI programs will be able to collect, process, and analyze new CTI sources seamlessly whenever necessary.
- **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 TIP 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 the noise 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 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 (i.e., firewalls, web threat gateways, proxies, etc.). 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. 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 many organizations. 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 threat reports, or providing managed and/or professional services for threat hunting.

Table 1. Threat Intelligence Requirements

Description	Details	Benefit
Growing range of CTI data	OSINT, commercial feeds, risk scores, reports, ISACs, etc.	Collect and synthesize CTI from multiple sources to help organizations keep up with and respond to threat actors, IoCs, TTPs, etc.
Central management and analysis platform	Threat intelligence platform designed to help organizations analyze, correlate, and manage large volumes of CTI	TIPs can be used to automate operations, normalize all threat data, and provide a consolidated interface for various users.
Customization options	Custom dashboards, notes, intel cards, etc.	Merges external CTI with internal security telemetry to accelerate investigations and remediation actions. Centralized TIP can be used by different types of users for individual use cases.
Advanced analytics	Machine learning, predictive analytics, etc.	Analytics acts as a "helper app" for security analysts and threat hunters to help reduce CTI noise, identify real threats, and accelerate IR and risk mitigation.
Technology integration	TIP integration with SIEM, GRC, firewalls, gateways, proxies, etc.	CTI solution interoperability can support SOAPA to streamline security operations and accelerate threat detection and incident response.
Support services	Managed services and/or professional services	Help organizations achieve best practices for CTI programs. Provide skills augmentation, additional resources, deep research reports, etc.

Source: Enterprise Strategy Group

Enter Recorded Future

In the past, CTI programs depended upon numerous technologies from an assortment of vendors, leading to the operations challenges described above. To address threat intelligence chaos, many organizations are rationalizing their CTI technology portfolios and replacing point tools with more consolidated CTI offerings.

CISOs looking for full-featured threat intelligence offerings may want to consider Recorded Future, a company whose mission is to organize the world's threat information and make it useful for organizations. Recorded Future aligns with the requirements described above, offering:

- A wide variety of threat intelligence information. Recorded Future already provides an assortment of OSINT, commercial threat intelligence feeds, government/industry threat data, technical and dark web data, etc. Recorded Future continually adds to these sources through the work of its own analyst and data teams as well as industry partnerships.
- A platform for CTI centralization. Organizations can store, access, and manage all their threat intelligence through the Recorded Future web application.
- Options for customization. Recorded Future can be customized for different user types including incident responders, threat hunters, vulnerability managers, and security executives. The company also added new features recently that allow organizations to integrate their own intelligence sources, creating threat intelligence notes to empower teams to collaborate, enhance investigations, train junior analysts, or create remediation policies.
- A foundation of machine learning. To help customers operationalize CTI, Recorded Future has added advanced analytics to its platform, helping customers identify high priority threats that deserve immediate attention.
- Numerous technology integration partners. Recorded Future has integration partners across technologies like SIEM, incident response platforms (IRPs), ticketing systems, advanced analytics, and security infrastructure players to deliver CTI to teams where they need it.
- Managed and professional services. To augment its customers' in-house staff, Recorded Future offers intelligence services (i.e., product onboarding, analyst support, quarterly reviews, etc.), integration services (i.e., workflow automation, data curation and ontology development, connectors for security tools and applications, etc.), training services, analyst services, and "elite research" services (i.e., threat experts, custom research, etc.).

Throughout its history, Recorded Future has evolved into a one-stop-shop for threat intelligence, combining key features from feeds, reports, providers, and platforms. As such, security leaders should consider how Recorded Future can help them tame threat intelligence chaos, consolidate technology, streamline operations, and improve ROI on threat intelligence programs.

The Bigger Truth

Based upon years of research and experience, leading organizations get the most out of their CTI programs by collecting diverse threat intelligence data, centralizing this data through a common platform, utilizing advanced analytics to make sense of CTI, and integrating CTI analysis with other technologies to speed and improve processes.

Getting to this point is often a learning experience whereby organizations live through threat intelligence chaos, develop a strategy for improvement, and then consolidate and integrate CTI technologies over time.

Historically, this was the only way to proceed, but this is no longer the case due to the onset of full-function CTI solutions from vendors like Recorded Future. CISOs looking for a faster way to improve threat intelligence operations and program ROI should contact Recorded Future and see how it aligns with their security objectives and requirements.