Solution Showcase

An All-Source Approach to Threat Intelligence Using Recorded Future

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

Abstract: When it comes to cyber threat intelligence (CTI), there is good and bad news for organizations. The good news is that security teams understand the value of threat intelligence programs and are increasing investments to maximize benefits. The bad news is that they continue to use threat intelligence tactically, making it difficult to operationalize threat intelligence to reach its potential. What's needed? An all-source approach that helps organizations use a wide range of threat intelligence to mitigate business risk, accelerate incident response, and streamline security operations. Recorded Future can help organizations achieve these goals.

Overview

Many organizations have established new threat intelligence programs or bolstered existing ones over the past few years. Why? Because threat intelligence is used as part of a growing number of risk management processes and security best practices. According to ESG research, 30% of enterprises say that threat intelligence collection/analysis practices are well established in their industry, 29% are interested in sharing threat intelligence within their industry, 25% believe that threat intelligence can help them prevent inbound attacks from malicious IP addresses, and 25% feel that threat intelligence may accelerate the time it takes for incident detection.[1]

Additionally, many organizations have further plans for threat intelligence programs in the future. For example:

- In a 2017 ESG research study, 28% of organizations said they collect substantially more data to support cybersecurity analytics and operations than they did two years ago, while another 49% claim they collect somewhat more data to support cybersecurity analytics and operations. Much of this data is open source, commercial, and industry-centric cyber threat intelligence.[2]
- Twenty-seven percent of organizations planned to significantly increase spending on their threat intelligence programs from 2015 to 2017, while another 45% said they would increase spending on their threat intelligence programs somewhat over the same timeframe. Increased investment includes purchasing threat intelligence feeds and tools, hiring more threat analysts, and providing additional training to the existing cybersecurity staff.
- Organizations have a list of other ambitious objectives for their threat intelligence programs. For example, 33% want to improve risk management efficiency and effectiveness, 31% want to use threat intelligence to automate

[1] Source: ESG Research Report, *Threat Intelligence and Its Role Within Enterprise Cybersecurity Practices*, June 2015. All ESG research references and charts in this solution showcase have been taken from this research report, unless otherwise noted.
[2] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.

remediation tasks, 25% want to establish a central threat management service for business units, and 23% want to leverage threat intelligence for proactive threat hunting.[3]

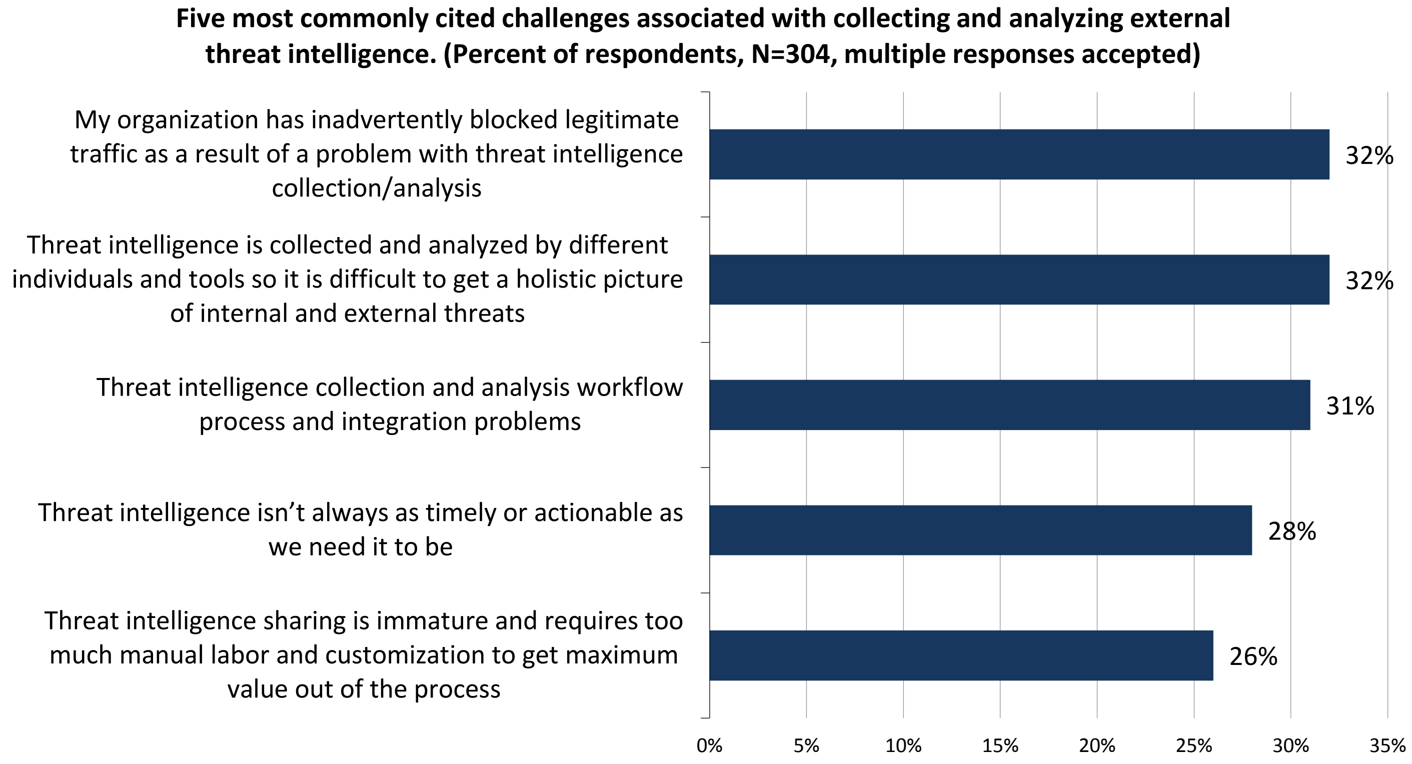
Threat Intelligence Programs Remain Immature

While many organizations have growth plans for their threat intelligence, these initiatives remain immature today—40% of organizations claimed that their threat intelligence programs had been in place for two years or less in 2015. Given this early stage of threat intelligence adoption, it comes as no surprise that cybersecurity teams experience several threat intelligence program challenges (see Figure 1). For example:

- Thirty-two percent have blocked legitimate traffic because of a problem with threat intelligence collection or analysis. This indicates a lack of understanding of threat intelligence and/or inaccurate sources.
- Thirty-two percent say that threat intelligence is analyzed by different people so it is difficult to get a holistic picture of the threat landscape. This indicates that it can be difficult to get a comprehensive perspective on threat intelligence and make it actionable for operations.
- Thirty-one percent report problems with threat intelligence workflow processes and/or integration. This makes it difficult to act upon threat intelligence proactively or use threat intelligence to improve the efficacy of other security technologies.

In summary, many CISOs appreciate the potential and value of threat intelligence programs, but some organizations still find it difficult to operationalize threat intelligence in a timely manner. Clearly, these firms need a more thoughtful and comprehensive threat intelligence strategy if they hope to maximize possible benefits.

Figure 1. Top Five Challenges Associated with Threat Intelligence Collection and Analysis



Five most commonly cited challenges associated with collecting and analyzing external threat intelligence. (Percent of respondents, N=304, multiple responses accepted)

Source: Enterprise Strategy Group

[3] ibid.

An All-Source Approach to Threat Intelligence

Too many organizations approach threat intelligence programs in an extremely tactical manner as analysts search for basic data, often indicators of compromise (IOCs) such as malicious IP addresses, domains, and URLs. Other firms simply equate threat intelligence with updated rule sets for security technologies like antivirus software, incident detection/prevention appliances (IDPs), or firewalls. These naive methods lead to threat intelligence program challenges and limited benefits.

Smart CISOs eschew this tactical method, opt for an all-source approach, and use threat intelligence in two distinct ways:

- **Strategic threat intelligence usage.** In this case, organizations use threat intelligence to provide tangible benefits to the business by identifying specific business risks. Some examples include protecting key individuals (e.g., executives, board members, visible individual contributors, etc.) and key corporate (IT) assets from exploits and compromises. This can be accomplished by three things: (1) using threat intelligence to identify and track cyber-adversaries, (2) monitoring chat sites to determine their motives and tactics, and (3) mining the dark web for credentials exposure related to identity theft. The strategic goals here are simple: Mitigate risks associated with cyber-attacks that could disrupt business operations (i.e., a DDoS attack) or damage an organization's reputation—ideally before the business is impacted.
- **Operational threat intelligence usage.** This fits into the classic use case for threat intelligence, but leading organizations take advantage of threat intelligence proactively in core security functions, such as patch prioritization, incident detection, scoping, and response. For example, most organizations use threat intelligence to look for common software vulnerabilities (CVEs) from open sources like NIST's national vulnerability database (NVD). This will produce a list of vulnerabilities, but how do cybersecurity professionals know which ones to prioritize? All-source threat intelligence practices can help here as analysts look for which vulnerabilities have known exploit kits, which ones have been used in active cyber-attacks, and which of these cyber-attacks are aimed at the organization's industry. Digging deeper with threat intelligence can help organizations sort through the cacophony of cybersecurity and help them identify where to focus scarce resources.

Other operational threat intelligence use cases include improving the communication of threat landscape awareness whereby security analysts track external cybersecurity trends from social media, paste sites, code repositories, and the dark web, and then share them with business and IT professionals. Finally, operational threat intelligence can also include integrating machine-readable threat intelligence with security analytics and controls. This can help add external context to internal security analytics to help improve decision making or automate controls and remediation by transforming newly discovered IOCs into security enforcement rules like blocking IP addresses and URLs.

What's Needed for an All-Source Threat Intelligence Program?

A holistic approach to threat intelligence is needed and it is built on a foundation of:

- **Integration options with existing security products.** Threat intelligence analytics systems should support open APIs and provide threat intelligence in machine-readable standard formats such as STIX and TAXII. In this way, threat intelligence can accentuate internal security analytics systems like SIEM or be used for incident response automation actions like creating new firewall rules as threats emerge.
- **Tools and services for threat intelligence analytics**. Raw threat intelligence may provide some intriguing data points, but its value is greatly accentuated with the right analytics tools and services that contextualize and enrich threat intelligence. In this way, threat intelligence builds upon itself, turning data nuggets into campaigns and patterns that can be prioritized and acted upon. To maximize threat intelligence value, the threat analysis and SOC teams need tools like intuitive user interfaces for investigations, natural language processing for queries, and cloud-based artificial intelligence capable of personalizing threat intelligence for individual organizations to accelerate operations.

- **A combination of open, closed, and technical sources of intelligence to enable all-source analysis.** Gaining insight for business and IT domains demands collection, processing, correlation, contextualization, and analysis of a wide range of intelligence sources. This includes everything from security blogs, wikis, paste sites, code sharing repositories, hacker and criminal forums, and dark web sites, to government resources and commercial threat feeds focused on threat actor tactics, techniques, and procedures (TTPs), campaigns, and IOCs. In this way, CISOs can gain valuable threat intelligence to promote security awareness about business risks, identify specific threats "in the wild," make smart decisions about prioritization, and fine-tune granular technical controls to remediate imminent risks.
- **Integration options.** External threat intelligence should be combined with internal security telemetry from SIEM, endpoint security tools, vulnerability management, ticketing systems, incident response, security orchestration, deep analysis, and security infrastructure. In this way, organizations can compare internal and external security data to perform investigations, discover unknown threats, and contextualize security data for faster decision making.

All-source threat intelligence programs can be used by business, IT, and security personnel for risk mitigation and accelerated incident response. Within the cybersecurity team itself, holistic threat intelligence can provide value to threat analysts, SOC staff, incident responders, penetration testers, red teams, threat hunters, and security executives.

All-Source Threat Intelligence and Recorded Future

All-source threat intelligence programs synthesize a wide range of threat intelligence sources and help organizations speed time to incident detection and time to incident response while streamlining overall security operations. This is the exact mission of Recorded Future, a Somerville, Massachusetts-based security vendor.

Recorded Future's cloud-based threat intelligence products are used by its customers to:

- **Consolidate threat intelligence collection.** Recorded Future amalgamates wide-ranging open, closed, and technical sources of intelligence into a common platform, alleviating the need for organizations to find and synthesize this threat intelligence on their own. With its latest release, all threat intelligence including internal analysis, research notes, and proprietary data and feeds (including internal white lists, black lists, watch lists, etc.) can be integrated directly into Recorded Future. In this way, security analysts can centralize all types of threat intelligence, bolstering collaboration and efficiency.

- **Fast-track all types of cybersecurity analytics.** Recorded Future provides straightforward interfaces, custom rules generation, and query tools for security analysts focused on risk mitigation, threat research, incident response, etc. Recorded Future augments its machine-learning-based technology with its own threat researchers to help identify campaigns, threat actors, and tactics targeting specific organizations. The automation provided by Recorded Future helps analysts to connect the dots to rapidly reveal unknown threats.

- **Enhance existing security tools, processes, and personnel.** Customers use Recorded Future in several ways. For example, threat analysts gain insight into emerging threats, and many use the API set to integrate Recorded Future threat intelligence with SIEM platforms like Micro Focus ArcSight, IBM QRadar, and Splunk as well as endpoint security, vulnerability management, ticketing, and other systems for real-time context. Recorded Future threat intelligence is often included into incident response workflows so that security analysts can compare internal security alerts with "in-the-wild" activities while integrated threat telemetry can be tuned or customized for more high-fidelity alerting when correlated with internal data. Finally, Recorded Future can act as a bridge between security and IT operations to help them adjust security controls and decrease the attack surface. In addition to its product, Recorded Future can provide intelligence services, enabling customers to get a head start without having to recruit a whole team.

Recorded Future supplements its threat intelligence delivered as a service with a team of experts with deep experience in threat intelligence analysis from government and industry sectors. Organizations needing help with their threat intelligence programs can call upon Recorded Future for on-demand threat intelligence resources for reporting (on a range of topics) or to augment internal teams lacking the right staffing or skills. In this way, Recorded Future can act as a one-stop-shop, offering leading threat intelligence and expert CTI services.

The Bigger Truth

When it comes to threat intelligence, security teams often express a common frustration: They see the value and possibilities of threat intelligence but continue to struggle to operationalize threat intelligence to reach this potential. The truth is security without intelligence makes organizations reactive and increases risk.

Organizations must approach their threat intelligence programs with the realization that threat intelligence is a means to an end rather than an end in itself. They must transform their threat intelligence programs from tactical IOC-based data collection and manual analysis to an all-source holistic approach that can deliver strategic business and operational benefits.

This demands a wide array of open, closed, and technical sources of threat intelligence, tools and services for threat intelligence analytics, analytics automation, ease of use, and the ability to easily integrate threat intelligence with other security and IT operations investments. Recorded Future can help organizations create holistic threat intelligence programs incorporating an all-source approach, and reap the associated benefits.

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