ESG SHOWCASE

Sixgill and Threat Intelligence Program Modernization

Date: October 2020 **Author:** Jon Oltsik, Senior Principal Analyst and ESG Fellow

ABSTRACT: Threat Intelligence is a foundational cybersecurity component, yet too many organizations struggle with threat intelligence collection, processing, analysis, and response. To truly modernize their threat intelligence programs, CISOs must think creatively and not only address current challenges but also find ways to use threat intelligence more proactively though all cybersecurity processes and within all technology controls. Sixgill can help them achieve these goals.

Overview

According to ESG research, many organizations remain challenged by cyber-threat volume and sophistication as well as the tactics, techniques, and procedures (TTPs) used by cyber-adversaries. For example, in an ESG research survey, 63% of organizations reported that they believed that security analytics and operations was more difficult in 2019 than it was two short years previous.[1] Why? Forty-one percent of cybersecurity professionals said that security analytics and operations was more difficult because the threat landscape is evolving and changing rapidly. In other words, organizations can't keep up with cyber-threats as they continuously grow and evolve at a faster pace than their threat analysts can manage. This is especially problematic in areas like fraud and reputation protection that require a deep understanding of cyber-adversary chatter, hacker behavior, and the tools used in targeted cyber-attacks.

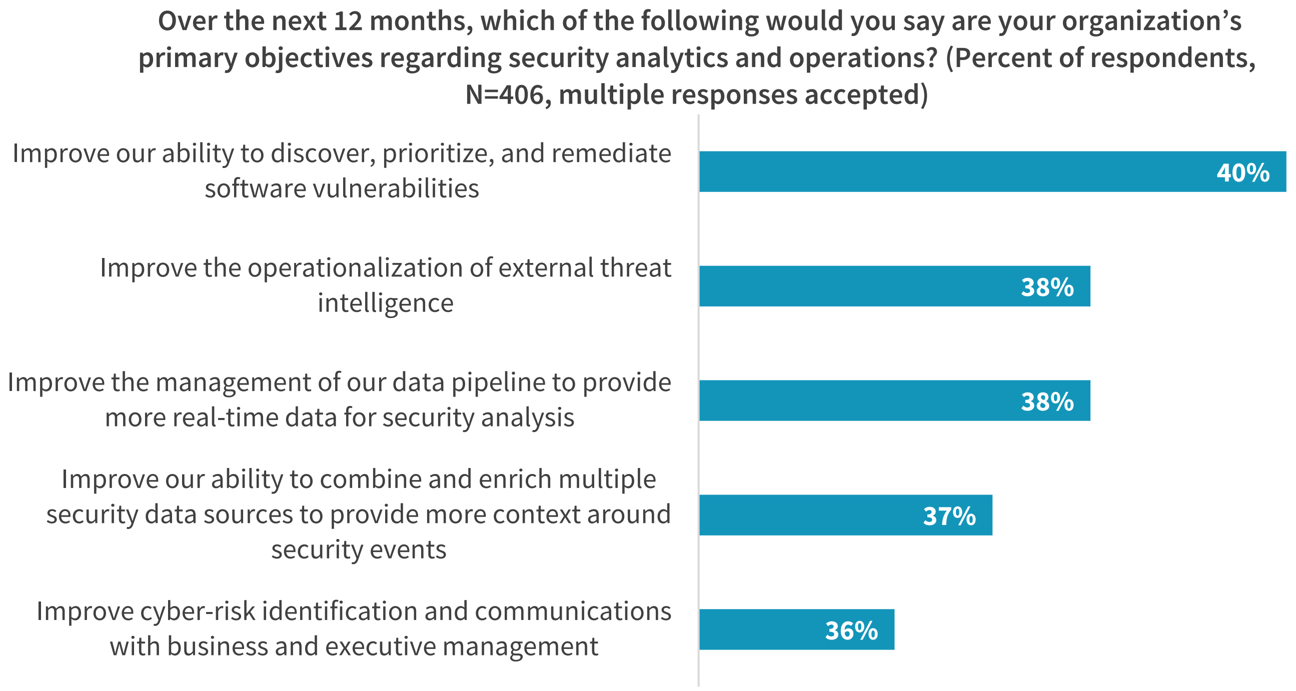
This gap should sound alarm bells as effective cyber-threat intelligence (CTI) analysis and operationalization are important components of an enterprise cybersecurity program, guiding risk and threat management efforts. This is evident in the ESG research. Cybersecurity professionals were asked to identify their organizations' primary objectives for security analytics and operations for 2020. Thirty-eight percent responded that their organization wanted to improve the operationalization of external threat intelligence, one of the top responses (see Figure 1).

It is also worth noting that the most common objective reported by respondents, improving the ability to discover, prioritize, and remediate software vulnerabilities, also depends upon threat intelligence analysis to understand which vulnerabilities have been exploited by threat actors in the wild. Furthermore, 37% of respondents claim that they want to improve their ability to combine and enrich multiple security data sources to provide more context around security events. Typically, this means enriching internal security telemetry like log or flow data with relevant and timely threat intelligence.

Overall, the ESG data indicates that while threat intelligence is an important component for cyber-risk and threat management, many organizations lack the right mix of threat intelligence people, processes, and technologies.

[1] Source: ESG Research Report, *The rise of cloud-based security analytics and operations technologies*, December 2019. All ESG research references and charts in this showcase have been taken from this research report, unless otherwise noted.

Figure 1. Top Five Security Analytics and Operations Objectives



Source: Enterprise Strategy Group

Threat Intelligence Analysis and Operationalization Challenges

Organizations recognize the importance of threat intelligence programs, so why do they continue to struggle? ESG sees a few common problems as many organizations:

- Rely on manual processes for data ingestion, analysis, and operationalization. Many firms gather open source and commercial threat intelligence from websites or serial data feeds and generic reports, then dedicate staff to analyze the data, find threats relevant to their business and IT infrastructure, input the data into SIEM systems, or translate indicators of compromise (IoCs) into blocking rule sets. These manual steps lead to lag time between threat discovery and subsequent preventative actions. Aside from being inefficient, manual processes can't scale to keep up with cyber-threat volumes or a growing enterprise attack surface.

- Are based on a myopic view of the threat landscape. Too often, threat intelligence is synonymous with IoCs like malware hashes, known phishing sites, or rogue IP addresses. Yes, these are important items that can be used to create blacklists, but they don't help organizations better understand who is attacking them and why.

- Have multiple resource gaps. While ESG research demonstrates that organizations appreciate the value of a strong threat intelligence program, many lack the right processes, staff, and skills to achieve their goals. It is also difficult to hire experienced threat intelligence analysts due to the global cybersecurity skills shortage.

- Consume and analyze threat intelligence in silos. Many security teams consume and analyze threat intelligence as part of various subgroups responsible for things like vulnerability management, security operations, or incident response, leading to inefficiencies and high costs. This siloed approach also leads to misjudgments—the VM group focused on Windows desktops may dismiss an open source software (OSS) threat as irrelevant without sharing it with an application development team using OSS components for a new application.

Additionally, organizations are collecting, processing, and analyzing large and growing volumes of threat intelligence. Many are struggling to scale operations to address this data explosion.

What's Needed?

It's time for organizations to take a more holistic approach to threat intelligence analysis and operationalization through centralization and end-to-end integration into their security programs. To do so, security teams must:

- Extend their threat intelligence purview. Beyond basic IoCs, large organizations should review other intelligence sources like social networking sites and deep/dark web chatter. This data can help threat analysts investigate who is attacking the organization, what types of tools they use, and how they tend to operate. By answering these questions, SOC teams can be more proactive in predicting and preventing threats while cyber-adversaries are still in the planning stages of their attacks.

- Automate threat intelligence from end to end. Rather than a series of manual steps, modern threat intelligence programs should be supported by machines and not just people. In other words, organizations should have access to a massive data lake of enriched threat intelligence that can be customized and automated for their specific data ingestion, analysis, and operating needs. In this way, they can focus on relevant threats to their business, industry, and geography without all the traditional manual overhead.

- Democratize threat intelligence across tools and processes. Rather than a siloed approach, an enterprise threat intelligence program should be set up as a service for all security requirements. To meet this need, organizations need a comprehensive portal where different analysts can create customized feeds, enrich the data, and operationalize threat intelligence for optimal and timely protection.

- Create a threat intelligence technology architecture built for integration. Ideally, threat intelligence should be tightly integrated with security controls like endpoint security, firewalls, and network proxies, as well as security operations systems like SIEM and SOAR. In this way, threat intelligence becomes a foundational element of processes for risk management and threat prevention, detection, and response.

- Utilize a common threat intelligence portal. To enhance investigations and threat hunting, SOC and threat intelligence analyst teams can benefit from a common threat intelligence portal so they can query and analyze raw data from a shared data lake.

Given the current situation, many CISOs will need guidance as they attempt to mature their cyber-threat intelligence programs. Sixgill may be a good source for help here. Taking a page out of agile development and DevOps, Sixgill promotes a concept it calls continuous investigation/continuous protection (CI/CP). CI/CP is based upon comprehensive automation of the entire threat intelligence program lifecycle, helping security teams collect, monitor, research, and respond after each intel development as seamlessly as possible.

CI/CP starts by monitoring a wide variety of threat intelligence including the deep/dark web, social networks, etc. The goal here is to track hacker chatter and actions in their genesis phase, before they turn into actual targeted attacks. By doing so, Sixgill enables its customers to "shift left" and react to threats before they are executed. Beyond this early threat reconnaissance, Sixgill can enable a modern threat intelligence program by providing:

- A threat intelligence data lake that is enriched automatically based upon an organization's industry and IT infrastructure, as well as the threats it faces.

- Curated and predictive indicators that can be shared with SIEM systems for investigations or SOAR tools to implement automated remediation playbooks.
- An investigations portal where threat and SOC teams can further analyze the intelligence.
- A central hub providing threat intelligence to all security tools and processes for activities like vulnerability management, security operations, incident response, etc.

Sixgill offers intelligence collection, enrichment, aggregation, monitoring, investigations, response, and remediation. In other words, Sixgill can help organizations modernize threat intelligence programs and improve risk management and threat management, as well as incident response, efficacy, and efficiency.

The Bigger Truth

Threat intelligence programs won't become more effective or efficient on their own, and tactical changes will only produce marginal benefits. Rather than taking inadequate steps, it's time that CISOs reimage their threat intelligence programs and integrate them into all aspects of cybersecurity processes.

Sixgill and its CI/CP model can help here by shifting threat intelligence left, early in the progression of cyber-attacks. Furthermore, Sixgill is designed to help throughout the threat lifecycle across data collection, ingestion, processing, analysis, and response. In this way, Sixgill can help organizations modernize their threat intelligence programs and improve their overall cybersecurity posture.

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

www.esg-global.com contact@esg-global.com 508.482.0188