SOLUTION SHOWCASE

Keys to Operationalizing Threat Intelligence

Date: September 2016 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: Enterprise organizations are increasingly using threat intelligence programs to help them in areas like network security, incident response, supply chain management, and centralized threat intelligence analysis. Many firms are also increasing their spending on threat intelligence programs while collecting, processing, and analyzing additional threat intelligence feeds. In spite of these positive steps, however, threat intelligence programs are often immature and challenging.

This ESG Solution Showcase outlines four keys to operationalizing threat intelligence programs for better security and operations.

Overview

According to ESG research, enterprise organizations are establishing cyber-threat intelligence programs to support their risk management and cybersecurity strategies.[1] For example:

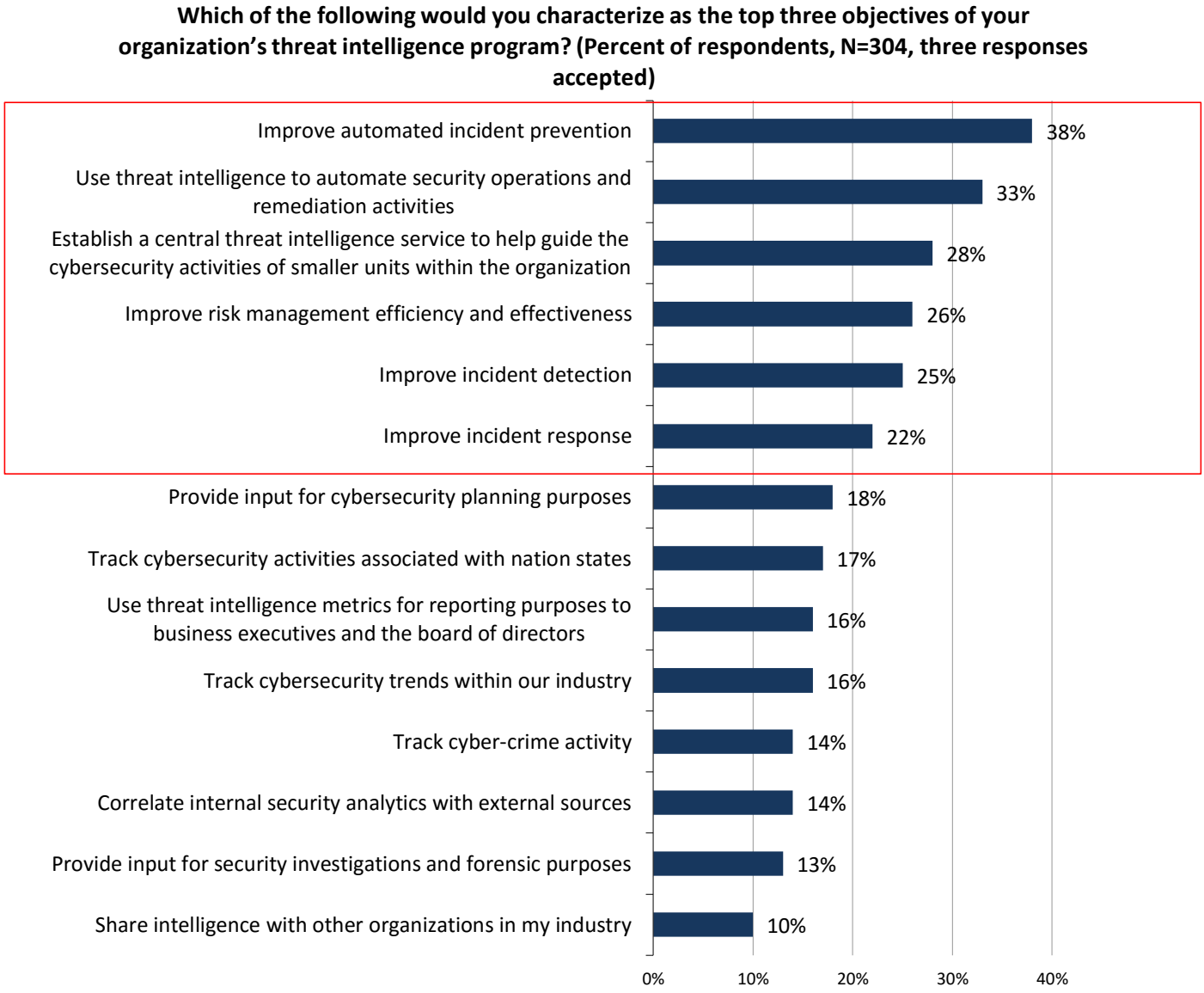
- 72% of enterprise organizations plan to increase spending on their threat intelligence programs over the next 12 to 18 months.
- 60% of enterprise organizations claim that 26 employees or more review threat intelligence as part of their day-to-day responsibilities.
- 69% of enterprise organizations report regular use of six or more different external threat intelligence sources as part of their threat intelligence programs.
- 55% of enterprise organizations plan to collect, process, and analyze additional external threat intelligence over the next 12 to 24 months.

CISOs are investing in threat intelligence programs for many reasons. The research states that the most-cited objectives for threat intelligence programs include improving automated incident prevention, using threat intelligence to automate security operations and remediation activities, and establishing a central threat intelligence service (see Figure 1).

Overall, according to the most-cited half dozen objectives, security teams are focusing on becoming more efficient and effective at incident prevention, detection, and response.

[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.

Figure 1. Threat Intelligence Program Objectives



Source: Enterprise Strategy Group, 2016

Threat Intelligence Programs Are Immature and Challenging

While enterprise organizations are embracing threat intelligence programs with the best of intentions, ESG research points to numerous problem areas. First, most threat intelligence programs are relatively new—ESG research indicates that 40% of enterprise organizations have had their threat intelligence program in place for less than two years. Given this relative immaturity, it is not surprising that many firms continue to struggle when it comes to turning threat intelligence data into cybersecurity actions and measurable results. For example, ESG research points out numerous threat intelligence program challenges (see Figure 2):

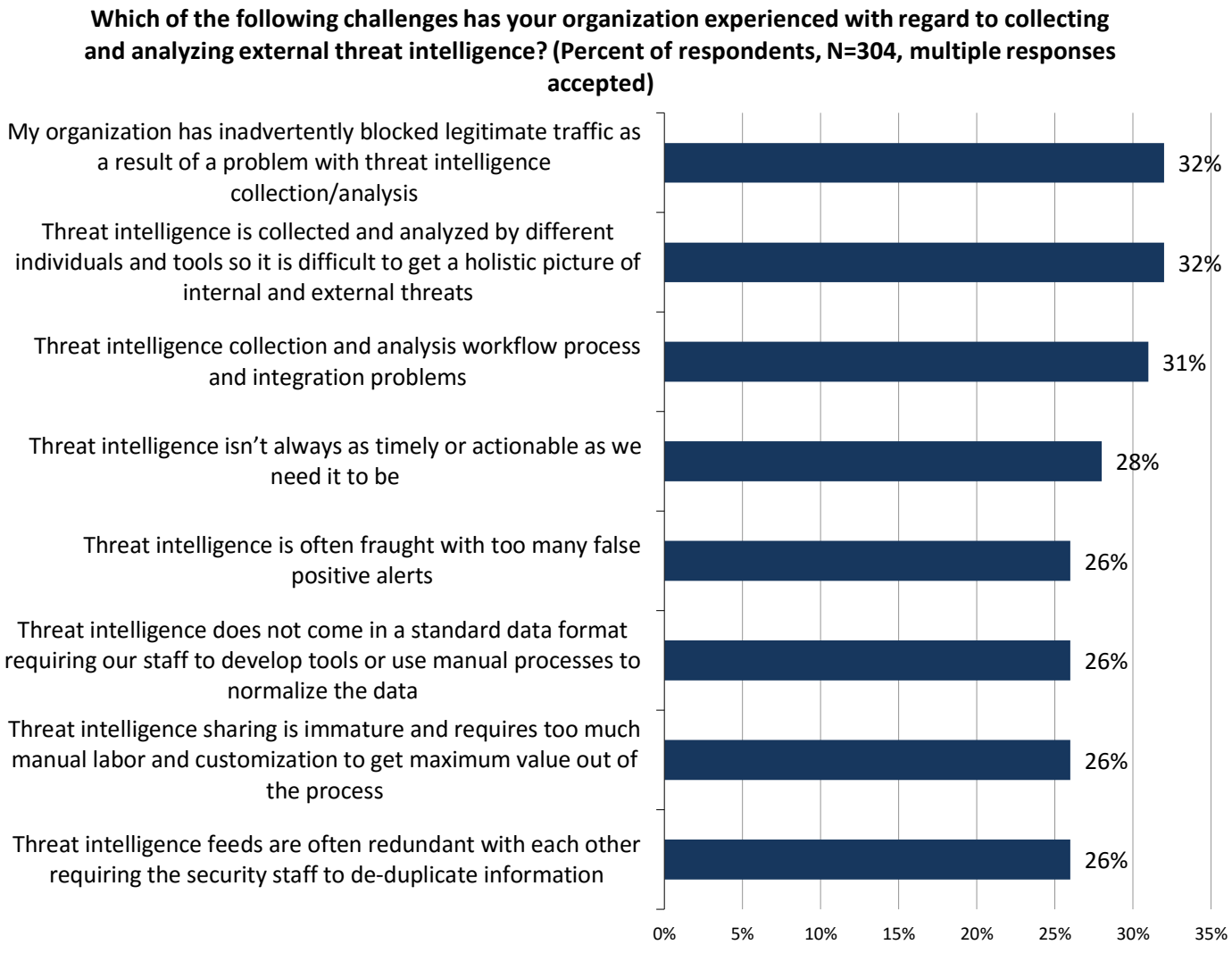
- Nearly one-third (32%) of organizations have inadvertently blocked legitimate traffic as a result of a problem with threat collection and/or analysis. This indicates that organizations haven't established the right skills and processes for threat intelligence analysis, leading to false positives and business disruption.

- Another 32% of organizations claim that threat intelligence is collected and analyzed by different individuals and tools so it is difficult to get a holistic picture of internal and external threats. This points to organizational and process issues that continue to hinder threat intelligence analysis and strategy.

- Thirty-one percent of organizations point to threat intelligence collection and analysis workflow process and integration problems. This indicates process and technology issues that limit the ability of cybersecurity groups to turn threat intelligence into remediation actions for incident response and risk management.

- More than one-quarter (28%) of organizations lament that threat intelligence isn't always as timely or actionable as they need it to be. These firms may be collecting the wrong threat intelligence or struggling with the workflows necessary to actually act upon high-priority threat intelligence.

Figure 2. Threat Intelligence Challenges



Source: Enterprise Strategy Group, 2016

CISOs have worthwhile threat intelligence program goals but today's results are marginal at best. Clearly, a lot of work remains.

Operationalizing Threat Intelligence

As part of its threat intelligence research project, ESG heard a common refrain: CISOs talked about the need to improve the operationalization of threat intelligence in order to maximize benefits. What exactly does this entail? ESG believes that operationalizing threat intelligence involves four key components:

1. **Improving threat intelligence quality.** Enterprise organizations certainly consume a lot of threat intelligence feeds, but unfortunately, much of this so-called "intelligence" is out-of-date or basic data about malicious IP addresses, domains, and URLs. Much of this pedestrian data is also highly redundant, delivered in every independent threat feed and intelligence update integrated into threat management technologies. Little wonder why 72% of cybersecurity professionals believe that about 50% to 100% of all the data contained in threat intelligence feeds is redundant regardless of the source. What's needed is timely, high-fidelity threat intelligence that aligns with an organization's business processes, location, vertical industry, supply chain partners, etc. Rather than buying an assortment of generic threat intelligence feeds, CISOs must put in the time to customize threat intelligence to their unique needs. By putting the work into building a portfolio of customized threat intelligence, CISOs can actually eliminate a lot of existing low-quality threat intelligence they currently pay for and establish a central repository of high-quality threat intelligence to be used for all threat intelligence analysis and actionable remediation needs across the enterprise.

2. **Consolidating threat intelligence analysis into a common platform.** As previously mentioned, threat intelligence is often consumed and analyzed by different individuals and groups, creating a situation of threat intelligence Balkanization. As an alternative, large organizations should point all threat intelligence to a centralized threat intelligence platform that acts as a hub for data collection, normalization, management, and analysis. Threat management analytics should offer manual query capabilities while providing big data machine learning algorithms to help analysts improve threat detection, forensic investigations, and prioritization.

3. **Integrating threat intelligence with internal security monitoring systems.** Threat intelligence platforms should be viewed as a hub-and-spoke architecture. Threat intelligence feeds are centralized to improve analysis and management. Once this occurs, however, threat intelligence must be shared with an array of security analytics systems (i.e., SIEM, network security monitoring, endpoint monitoring, etc.) to compare external threat intelligence with internal network activities.

4. **Using threat intelligence for real-time risk mitigation.** In addition to security monitoring and analysis, strong security depends upon turning threat intelligence warnings into remediation actions. This demands tightly coupled integration between threat intelligence platforms and perimeter security enforcement points like firewalls, IDS/IPS, web and email security gateways, and recursive DNS services. The goal here is remediation process automation. When threat intelligence detects a malicious command-and-control (C2) server, it can create a firewall rule or use DNS intelligence to block an external connection. This type of real-time remediation automation can not only bolster cybersecurity defenses but also streamline security and network operations.

LookingGlass Cyber Solutions' Comprehensive Approach to Threat Intelligence

Operationalizing threat intelligence depends upon tightly integrated security technologies and coordinated organizational processes, but this level of synchronization is often lacking at large organizations. Most often, CISOs base their threat intelligence programs on a myriad of threat feeds and technologies from assorted vendors, leading to disorganization, high costs, and an integration nightmare.

LookingGlass Cyber Solutions is one of few companies that can help CISOs alleviate this threat intelligence program chaos as it offers products and services that align well with the four components for threat intelligence operationalization described above, including:

- **High-fidelity threat feeds.** LookingGlass provides threat data feeds in the form of machine-readable threat intelligence from hundreds of sources that can be customized for each organization based upon location, industry, supply chain partners, etc. In December 2015, LookingGlass bolstered its threat intelligence data capabilities with the acquisition of Cyveillance, a market leader. Post-acquisition, LookingGlass now offers threat intelligence in many forms including feeds around historical and active infection records, known command-and-control (C2) server activities, known malicious URLs observed serving malware, known phishing URLs, newly registered domains, and access to a database of compromised account credentials totaling over two billion unique username and password combinations.

- **Threat intelligence platforms.** LookingGlass offers multiple on-premises and SaaS-based solutions that extract, transform, and load its threat intelligence feeds into common platforms for analysis. LookingGlass also correlates data from social media, web searches, and dark web channels to monitor for threats to specific industries and organizations. The ScoutVision, ScoutPrime, and Cyber Threat Center (CTC) threat intelligence platforms are also built for integration with existing security tools like SIEM and network enforcement points for internal/external monitoring and analysis as well as security remediation operations. ScoutInterXect correlates internal, customer-specific network telemetry with both historical and real-time threats identified in ScoutVision and located on the global Internet.

- **Threat mitigation.** LookingGlass offers its own threat mitigation appliances already tightly integrated with its global threat intelligence. NetDefender threat mitigation appliances integrate malware defense and balance the needs of network and security architects by delivering a stealthy security enforcement point that also transparently replicates traffic to third-party sensors to accelerate remediation actions while protecting existing investments in security products and preserving network bandwidth. LookingGlass DNS Defender threat mitigation appliances are protocol-specific firewalls that protect against DNS attacks, accelerate DNS performance, and provide insight into DNS traffic. LookingGlass also offers its NetSentry appliances that deliver a high-performance, enterprise-grade Network Intrusion Detection System (NIDS) that combines industry-standard SNORT IDP signature-based technology with LookingGlass Deep Packet Processing (DPP).

- **Threat intelligence services.** LookingGlass Services provides cybersecurity experts with advanced threat intelligence tools to augment an organization's security staff or to assist with special projects (i.e., brand protection, rogue application or phishing take downs, executive threat assessment, and mitigating compromised credentials).

The Bigger Truth

Threat intelligence consumption and sharing make a lot of sense for cybersecurity improvement. Effective threat intelligence consumption can help organizations compare internal network and system behavior with known threats "in the wild," while threat sharing can help communities of interest benefit from their collective experiences via the "network effect."

While threat intelligence consumption and sharing make intuitive sense, threat intelligence benefits really depend upon efficient and effective threat intelligence programs. Unfortunately, many organizations haven't achieved this level as threat intelligence remains immature and fraught with challenges.

ESG believes that operationalizing threat intelligence depends upon four components: High-fidelity threat feeds, consolidated threat intelligence platforms, threat intelligence integration with security monitoring systems, and using threat intelligence for automated remediation.

CISOs should assess their threat intelligence programs in each of these areas and address high-priority shortcomings. The goal is to create an end-to-end system to operationalize threat intelligence, improving security analysis and remediation process efficiency. With modular, scalable, and integrated solutions in each area, LookingGlass Cyber Solutions can help enterprises better operationalize threat intelligence within existing infrastructures and operations.

A good place to learn more is to listen to the ESG/LookingGlass webinar on "Operationalizing Threat Intelligence," which is available on demand at www.lookingglasscyber.com/resources.