Solution Showcase

Operational Threat Intelligence: Keeping Up with the Speed of Morphing Threats

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

Abstract: While many organizations are building and investing in threat intelligence programs, they face numerous challenges. In fact, one of the biggest issues is simply keeping up with constantly changing threats and turning threat intelligence into security operations actions. ESG recommends a four-point strategy for operationalizing threat intelligence, including improving threat intelligence quality, consolidating threat intelligence into a common platform, integrating threat intelligence with other types of security monitoring and analytics tools, and using threat intelligence to help automate processes for risk mitigation.

Overview

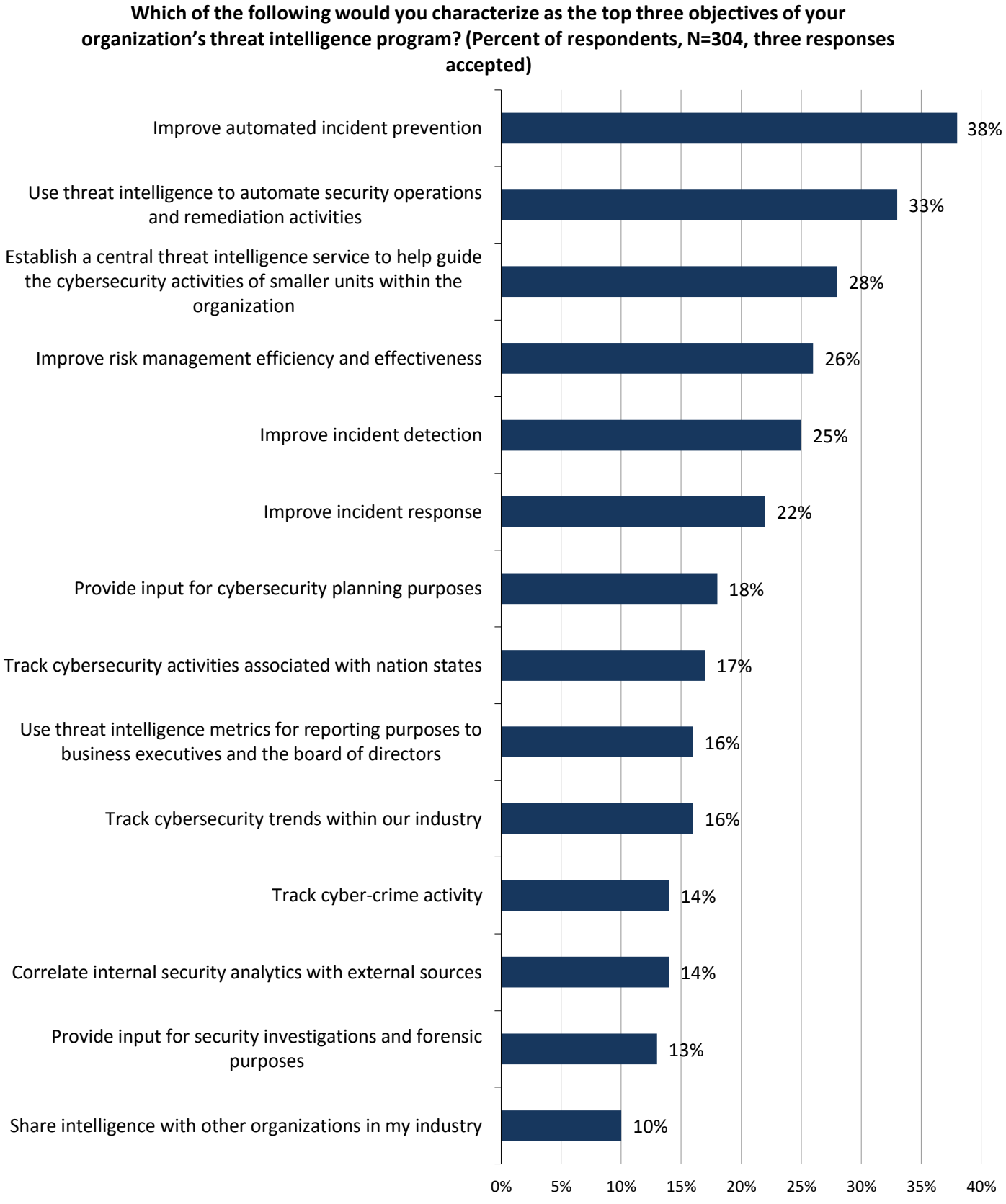
Threat intelligence programs have become an essential component of layered security defenses and ongoing security analytics. For example, ESG research indicates that:

- 72% of enterprise organizations plan to increase spending on their threat intelligence programs over the next 12 to 18 months.
- 55% of enterprise organizations plan to collect, process, and analyze additional external threat intelligence over the next 12 to 24 months.[1]

Why are organizations investing money on threat intelligence and collecting more threat intelligence data? According to ESG research, CISOs see threat intelligence as a means for achieving many objectives, including improving automated incident prevention, using threat intelligence to automate security operations and remediation activities, and establishing a central threat intelligence service for the entire enterprise (see Figure 1).

[1] Source: ESG Research Report, *Threat Intelligence and Its Role Within Enterprise Cybersecurity Practices*, June 2015. All other ESG research references and figures in this solution showcase have been taken from this report.

Figure 1. Threat Intelligence Program Objectives



Source: Enterprise Strategy Group, 2016

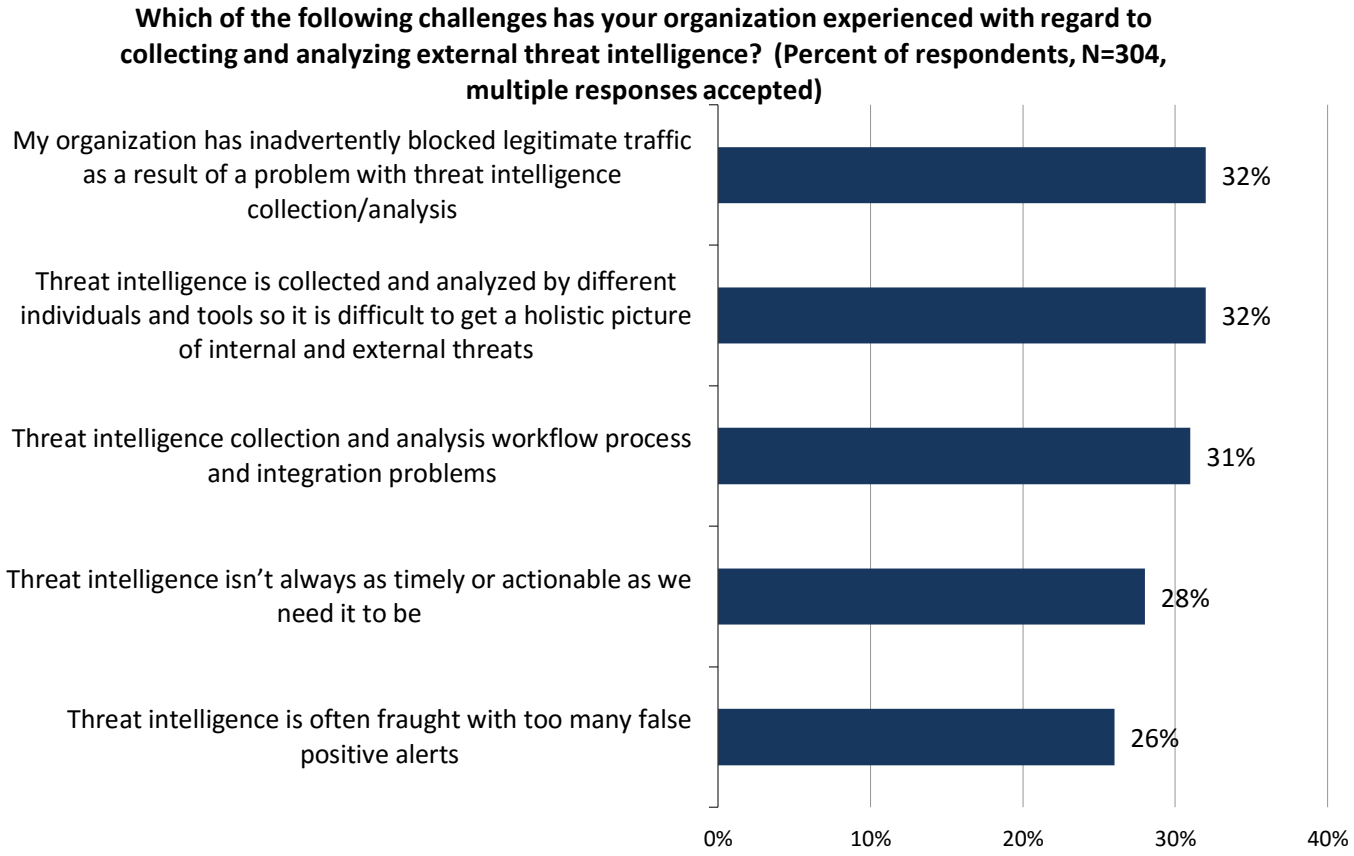
Threat Intelligence Programs Are Immature and Challenging

While organizations are investing in threat intelligence programs, it's important to recognize that many of these efforts are fairly recent and remain immature. In fact, ESG research shows that 40% of enterprise organizations have only had a threat intelligence program in place for less than 2 years. When asked about the maturity level of these programs, 56% of organizations characterize their threat intelligence programs as somewhat mature or somewhat immature, indicating a lot of work ahead.

Aside from immature threat intelligence programs, organizations also describe a number of specific challenges associated with collecting, processing, analyzing, and operationalizing threat intelligence. For example, (see Figure 2):

- 32% of organizations have inadvertently blocked legitimate traffic as a result of a problem with threat collection and/or analysis. This may indicate that organizations are having problems interpreting threat intelligence, correlating raw threat intelligence with their industries and organizations, or keeping up with rapidly-changing threats.
- 32% of organizations say 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 is especially troubling to CISOs responsible for communicating cyber-risk metrics to business executives and corporate boards.
- 31% of organizations describe challenges with threat intelligence collection and analysis workflow process and integration problems. This demonstrates basic problems associated with transforming raw data into information, insight, and action.

Figure 2. Top Five Threat Intelligence Challenges



Source: Enterprise Strategy Group, 2016

It is worth noting that 28% of organizations claim that threat intelligence isn't always as timely or actionable as they need it to be. This is especially troubling given much of the information highlighted in the Webroot 2016 Threat Brief titled *Next-Generation Threats Exposed,* published earlier this year. The Webroot Threat Brief indicates that the threat landscape is growing even more dynamic on a daily basis. For example:

- Nearly all malware and potentially unwanted application (PUAs) delivery uses polymorphism, making each variant unique. This leads to a frightening outcome–97% of malware instances in 2015 were unique to a single endpoint.
- Attackers using ransomware are increasingly adopting IP address anonymizing services such as TOR for ransomware delivery and cryptographic key positioning for each affected host. Anonymizing services makes it much more difficult to identify who is behind these types of attacks.
- Throughout 2015, the average number of net new malicious IP addresses increased from 85,000 to around 100,000 per day. Alarmingly, around 5% of the IP address entries change on a daily basis and 40% have never been associated with malicious behavior in the past.
- With the number of new URLs greatly increasing, it has become even more difficult to identify malicious and benign variations. Webroot regularly examines these URLs across 83 primary categories and assigns a reputation score to each one. Based upon this analysis, Webroot determined that online greeting cards, dynamically generated content, and marijuana URLs represent the riskiest categories in 2015.

Additionally, according to Webroot September Quarterly Threat Trends:

- In 2016, the number of phishing counts for Google and Wells Fargo sharply increased primarily due to the use of polymorphic URLs, thousands of sites with small variants from a single IP address, for phishing campaigns. Polymorphic URLs target numerous users at once while avoiding detection by traditional methodologies.
- The percentage of malicious mobile apps classified as adware or PUAs has skyrocketed in 2016. A sharp increase in adware containing rootkits is a concerning new trend.

Operationalizing Threat Intelligence

ESG research points to threat intelligence program immaturity and numerous challenges associated with operationalizing threat intelligence. One of the challenges highlighted uncovers the fact that many organizations have trouble keeping threat intelligence up to date since attackers' tactics, techniques, and procedures (TTPs) tend to change on a constant basis. In light of the Webroot threat intelligence findings, this situation will continue to degrade without proper attention.

Given the dynamic threat landscape, how can organizations possibly stay current with threats and operationalize today's immature threat intelligence programs? ESG recommends four key steps:

1. **Start by improving threat intelligence quality.** Enterprise organizations consume a lot of threat intelligence feeds but much of this "intelligence" is nothing more than basic data about malicious IP addresses, domains, and URLs. Much of the rudimentary threat intelligence is highly redundant, delivered in every independent threat feed and intelligence updates integrated into threat management technologies. What's needed is timely, high-fidelity threat intelligence that aligns with an organization's business processes, location, vertical industry, supply chain partners, etc.
2. **Consolidate threat intelligence analysis into a common platform.** The ESG research reveals that threat intelligence is often consumed and analyzed by different individuals and groups. To overcome this situation, large organizations

should consolidate threat intelligence to a centralized threat intelligence platform that acts as a hub for data collection, normalization, management, and analysis.

3. **Integrate threat intelligence with internal security monitoring systems.** Threat intelligence platforms should be viewed as a hub-and-spoke architecture. First, threat intelligence feeds are centralized to improve analysis and management. Once this occurs, however, threat intelligence should be shared with security analytics systems like SIEM, network security monitoring, endpoint monitoring, etc., in order to compare external threat intelligence with internal network activities.

4. **Use threat intelligence to help automate risk mitigation.** Strong security processes should transform timely threat intelligence into remediation actions. This demands tightly coupled integration between threat intelligence platforms and perimeter security enforcement points like firewalls, IDS/IPS, and web and email security gateways, as well as endpoint security controls. New threat intelligence around new malware variants, attacker TTPs, or malicious files, URLs, and IP addresses, can be consumed by existing security controls and immediately turned into prevention and detection rules to lower overall IT risk.

By taking these steps, CISOs should be able to greatly improve the effectiveness of their threat intelligence programs by keeping up with ever-changing threats, comparing threat intelligence with internal security analytics, and turning threat intelligence into automated action for risk reduction and mitigation.

The Bigger Truth

Many CISOs see the potential for threat intelligence consumption, analysis, and sharing as a means for improving threat prevention, detection, and response. This is certainly why so many enterprise organizations have established and continue to invest in threat intelligence programs.

While this is a step in the right direction, threat intelligence programs will offer marginal benefits at best if they can't keep up with the dynamic threat landscape. ESG believes that the four points outlined in this solution showcase can help organizations operationalize their threat intelligence efforts, leading to greater efficacy, efficiency, and lower IT risk.