Enterprise Strategy Group | Getting to the bigger truth.™

Solution Showcase

Webroot Cloud-based Machine Learning Can Help Organizations Operationalize Threat Intelligence

Date: November 2016 **Author:** Jon Oltsik, Sr. Principal Analyst

Abstract: Large organizations have jumped on the threat intelligence bandwagon as they establish threat intelligence programs, consume lots of commercial and open source threat intelligence feeds, and increase threat intelligence budgets. So, what's the problem? Many enterprises struggle to "operationalize" threat intelligence. In other words, they struggle to use threat intelligence to reduce risk, block threats, or fine-tune security controls in a timely manner. Cloud-based machine learning from Webroot can help here. Webroot BrightCloud services can deliver accurate and timely threat intelligence tightly integrated into an organization's security controls. This can help operationalize threat intelligence, accelerate remediation actions, and mitigate risk.

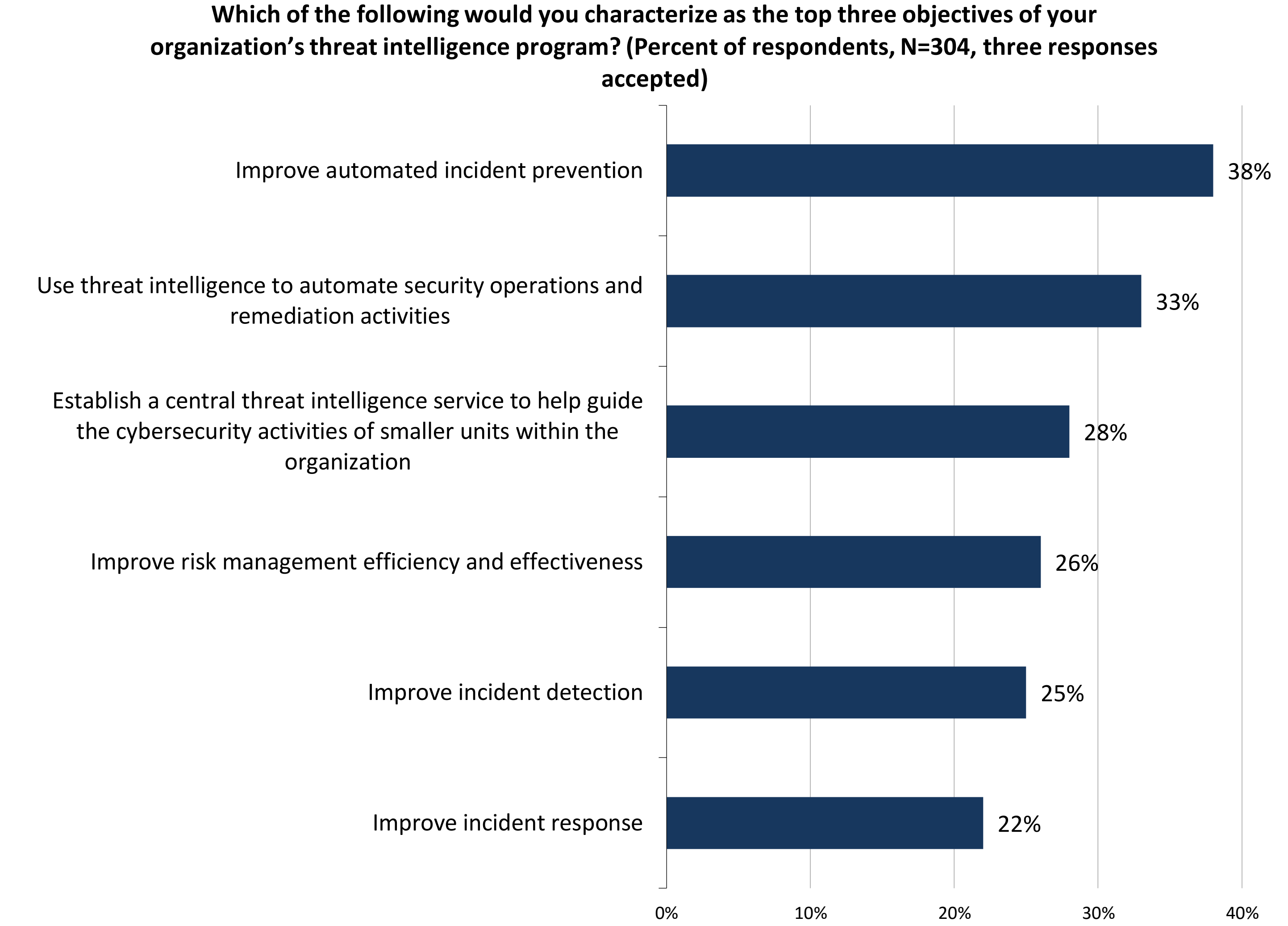
Overview

Enterprise organizations (i.e., 1,000 employees or more) are establishing and embracing threat intelligence programs. According to ESG research:

- Twenty-seven percent of cybersecurity professionals say that spending on their organization's threat intelligence program will increase significantly over the next 12 to 18 months while another 45% claim that spending on their organization's threat intelligence program will increase somewhat over the same timeframe.
- Fifty-five percent of enterprise organizations plan to collect, process, and analyze an increasing amount of external threat intelligence over the next 12 to 24 months.
- When asked to identify the top objectives for their organization's threat intelligence program, 38% stated that they want to improve automated threat prevention, 33% want to use threat intelligence to automate security operations and remediation activities, 28% want to establish a central threat intelligence service to help guide the cybersecurity activities of smaller units within the organization, and 26% seek to improve risk management efficiency and effectiveness (see Figure 1).[1]

[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 report, unless otherwise noted.

Figure 1. Top Threat Intelligence Program Objectives

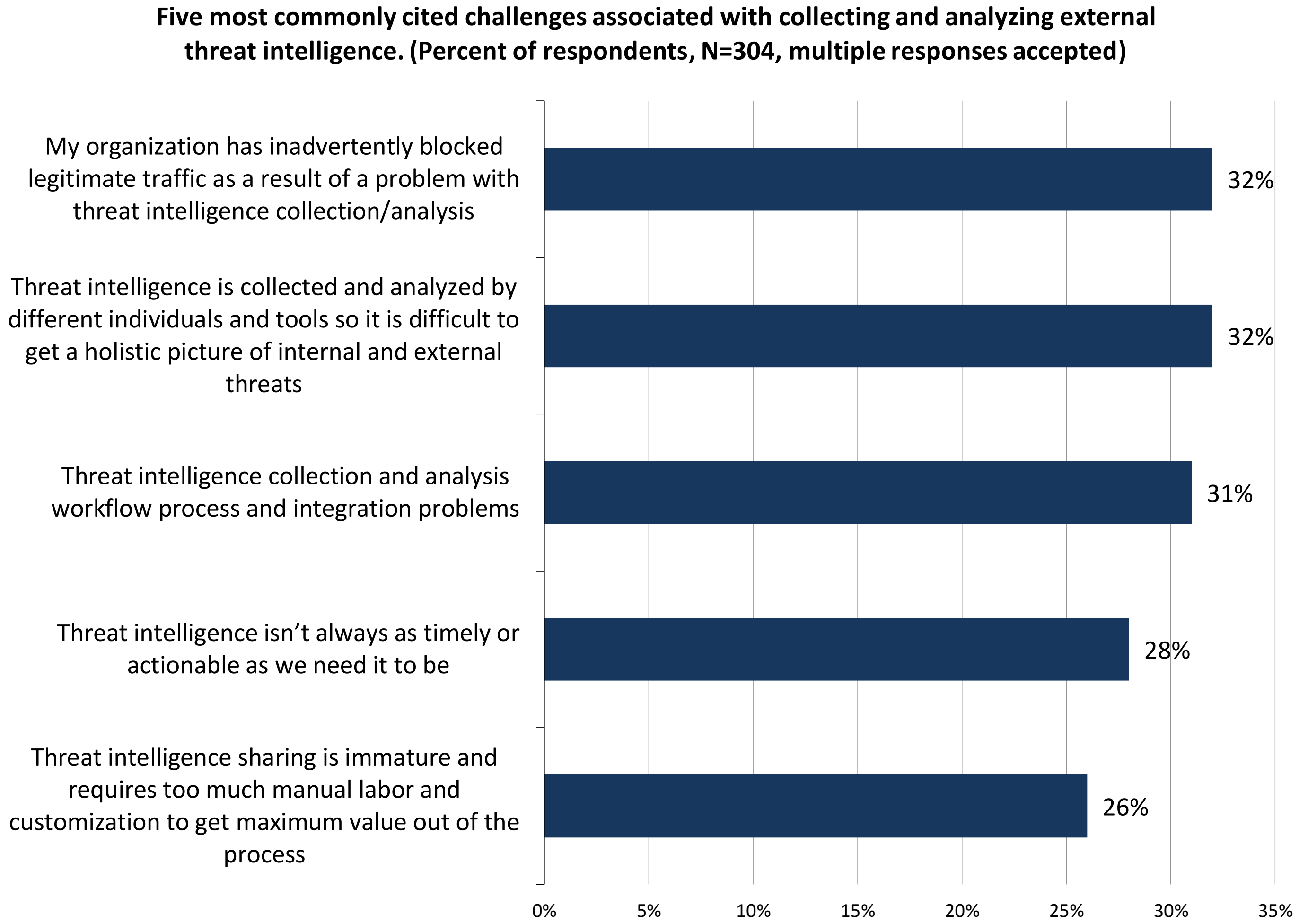


Source: Enterprise Strategy Group, 2016

Threat Intelligence Programs are Fraught with Operations Challenges

Although large organizations continue to build threat intelligence programs, many struggle to operationalize threat intelligence in a timely manner. In other words, enterprises find it difficult to sift through mountains of threat intelligence data, find the needles in haystacks that may impact their organization directly, and then act upon this threat intelligence to fine-tune security controls and block potential threats. In fact, cybersecurity professionals point to numerous threat intelligence challenges including misreading threat intelligence and then inadvertently blocking legitimate traffic, struggling to piece together a holistic view of the threat landscape, and handling problems associated with threat intelligence workflow processes and integration (see Figure 2).

Figure 2. Top Five Challenges Experienced with Threat Intelligence Collection and Analysis



Source: Enterprise Strategy Group, 2016

Threat intelligence operational challenges are also exacerbated by the global cybersecurity skills shortage. For example, ESG research indicates that 46% of organizations claim to have a problematic shortage of cybersecurity skills in 2016.[2] Furthermore, in a recently published research report from ESG and the Information Systems Security Association (ISSA), 63% of cybersecurity professionals say that while they try to keep up on cybersecurity skills, it is hard to do so given the day-to-day demands of their jobs.[3] This data indicates that many enterprise organizations are understaffed and under-skilled in cybersecurity, making it even more difficult to keep up with or operationalize threat intelligence in an optimal timeframe.

Improving Threat Intelligence Operations

When it comes to threat intelligence, enterprise organizations seem to be caught in a Faustian compromise. They understand that threat intelligence can provide timely intrinsic knowledge about the threat landscape but operational and staffing problems prevent them from taking full advantage of this information to improve security efficacy.

[2] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

[3] Source: ESG and ISSA Research Report, *The State of Cyber Security Professional Careers: An Annual Research Report (Part I),* October 2016.

So what's needed? To overcome current process bottlenecks, threat intelligence must be more accurate and timely. Accuracy here means not only identifying what's malicious and what's benign, but also providing some type of risk scoring around threats so individual organizations can make appropriate policy enforcement decisions. For example, a specific threat may target financial services organizations, so it might be categorized as very malicious to banks while appearing on a watch list for retailer and health care firms. In addition to accuracy, threat intelligence operations can gain efficiencies using machine-readable threat intelligence (MRTI) that is tightly integrated with actual security controls like firewalls, web threat gateways, AV gateways, and endpoint security software.

Webroot Cloud-based Machine Learning Can Help

Improving the operational efficiency of threat intelligence requires the ability to sort through and contextualize massive amounts of data, identify and score potential threats, and then distribute threat intelligence to security controls distributed across the global Internet. Thus, automating this process depends upon a massively-scalable big data architecture as well as leading data science algorithms that can quickly detect and categorize threats.

Webroot BrightCloud threat intelligence is designed to bridge the threat intelligence gap to help organizations operationalize threat intelligence through integrations with over 40 security vendors. These integrations provide real-time threat intelligence to security control like firewalls and web threat gateways. How? BrightCloud intelligence can accomplish this because it:

- **Is built for massive scale.** To keep up with the enormous threat intelligence volume, Webroot built a big data architecture similar to those used by Amazon, eBay, Facebook, and Twitter based on globally distributed AWS-based Cassandra database clusters that deliver massive scale and performance. This infrastructure allows Webroot to collect, process, classify, and analyze millions of new IP addresses, URLs, domains, and files that change constantly.

- **Uses advanced machine-learning techniques.** Through years of experience with machine learning, Webroot's models and algorithms are far more evolved than the plethora of commercial security analytics tools claiming machine learning capabilities. Why? BrightCloud machine learning capabilities start with massive data sets based upon its global endpoint security installed base, active scanning and crawling within the IPv4 space, passive Internet scanners, honeypots, and third-party lists. Webroot uses this large data set to generate and classify data features, model supervised and unsupervised learning, label event output, and then use feedback loops and researcher feedback to improve the models over time. Webroot also uses a fifth-generation active feedback model enabling BrightCloud services to reach model capacity much faster than older data science methodologies. In this way, Webroot can understand and visualize threat vectors across multiple domains in real time.

- **Provides a scoring system for threat intelligence accuracy and relevance.** Webroot's investment in machine learning provides accurate and timely threat intelligence to its customers. To accomplish this, BrightCloud services categorize all Internet objects and provide a reputation score for each one based upon a 100-point scale. For example, an object with a score of 50 to 60 could indicate that it was previously malicious or has the potential to become malicious in the future. This scoring system can help enterprises operationalize threat intelligence, helping them prioritize which threat intelligence to act upon, which to investigate further, and which to ignore.

- **Tightly integrates with existing network and endpoint security controls.** Webroot provides machine-readable threat intelligence that integrates directly with Webroot security products (i.e., endpoint security software, email security software, web security software, etc.) as well as third-party products from Webroot partners like A10 Networks, Aruba (HPE), Cisco, F5 Networks, Palo Alto Networks, and others. Once Webroot uncovers new threats, it shares this intelligence with policy enforcement controls, accelerating remediation and further reducing the attack surface.

The Bigger Truth

During 2015, Webroot saw hundreds of millions of new, unique executable files. Of these files, approximately 3.7% were determined to be malware, and 7.1% were identified as potentially unwanted applications (PUAs). Keeping track of this level of malicious activity can't be accomplished by ploughing through assorted commercial and open source threat intelligence feeds. This is likely why enterprise organizations have so many challenges operationalizing and benefitting from threat intelligence.

Facing millions of malicious threats on a daily basis, manual processes and incremental threat intelligence technologies simply aren't enough—enterprise organizations need help collecting, processing, analyzing, and classifying threat intelligence.

Webroot can help here, as its BrightCloud threat intelligence services are designed to accurately monitor, classify, analyze, and assess millions of Internet objects at all times. Beyond threat identification alone, Webroot also integrates its threat intelligence with a variety of on-premises security controls. This can help organizations operationalize threat intelligence by accelerating remediation actions.

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