ESG Brief

The Growing Need for Real-time and Actionable Security Intelligence

Date: February 2014 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: *ESG data indicates that many enterprise organizations are not only consuming commercial threat intelligence, but also using it to improve risk management. In fact, advanced organizations seem to include security intelligence as a best practice as they claim to get a lot of value from external security intelligence. While this is encouraging, the fact remains that not all security intelligence is created equally. New independent security intelligence services from providers like Norse are starting to emerge in the market. This type of intelligence can provide real-time, detailed intelligence focused on cybercriminal activities. Enterprise organizations can use this type of focused data to make timely risk management decisions, automate security operations, and improve incident detection/response.*

Overview

Large organizations are collecting more disparate security data feeds, keeping this data online for longer periods of time, and using the data for more types of security analysis and investigations. In spite of all this, internal data collection and analysis is no longer enough. To execute on strong risk management and timely incident detection/response, CISOs need to supplement internal data with highly relevant external security intelligence.

In fact, ESG research indicates that nearly two-thirds of surveyed enterprises use external threat intelligence as part of their information security analytics activities today (see Figure 1).[1]

Figure 1. Use of External Threat Intelligence as Part of Information Security Analytics Activities

Source: Enterprise Strategy Group, 2014.

[1] Source: ESG Research Report, *Emerging Intersection Between Big Data and Security Analytics*, November 2012.All other ESG research references and charts in this brief have been taken from this research report.

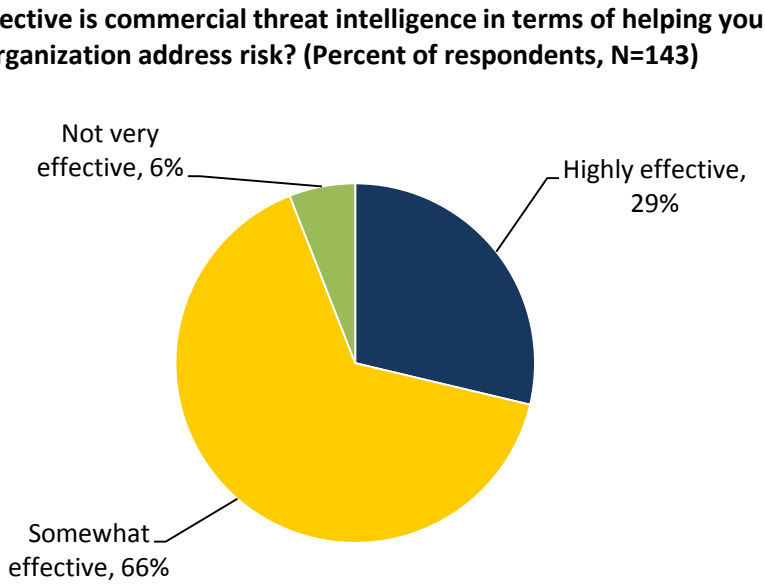
As part of its analysis, ESG used a scoring algorithm to segment the total survey population into three types of organizations: advanced (i.e., those with superior security processes, controls, and resources), progressing (i.e., those with average security processes, controls, and resources), and basic (i.e., those with below average security processes, controls, and resources). Using this segmentation model, 18% of enterprise organizations were classified as advanced, 56% were classified progressing, and 26% were classified as basic.

The ESG segmentation model is useful here because it indicates a varying use of external threat intelligence among the three segments: Ninety-five percent of advanced organizations use external threat intelligence as part of their information security analytics activities compared with 63% of progressing and 49% of basic organizations. Given this segmentation, it is safe to conclude that external security intelligence consumption and analysis can be seen as an enterprise security best practice.

External Security Intelligence Value

In theory, external threat intelligence should be extremely valuable if it is used proactively and effectively for improving risk management and incident detection/response. This thesis is consistent with ESG research findings. In total, 95% of surveyed organizations consuming external threat intelligence say that it is highly effective or somewhat effective (see Figure 2).

Figure 2. Effectiveness of Commercial Threat Intelligence to Help Organizations Address Risk



Source: Enterprise Strategy Group, 2014.

It should also be noted that there were strong differences of opinion between advanced, progressing, and basic organizations (see Table 1). Note that more than half (57%) of surveyed advanced organizations say that commercial threat intelligence is highly effective in helping their organizations address risk as compared with 43% of progressing and 0% of basic organizations. Based upon this data, it is safe to assume that advanced security organizations use security intelligence in a more meaningful way than other types of organizations, and this usage actually helps them improve risk management and cybersecurity responsiveness.

Table 1. Effectiveness of Commercial Threat Intelligence Analyzed by the ESG Segmentation Model

	Advanced	Progressing	Basic
Highly effective	57%	20%	15%
Somewhat effective	43%	76%	65%
Not very effective	0%	4%	19%

Source: Enterprise Strategy Group, 2014.

Analyzing Security Intelligence

Based upon ESG data, there is no question that enterprise organizations believe that external security intelligence can be extremely valuable in helping them manage IT risk more proactively. This makes sense since security intelligence is really meant to supplement internal security data with information about what's happening "in the wild." While it is safe to conclude that all security intelligence can be helpful, this raises a logical question: Is there certain security intelligence available that provides more value than others?

ESG believes that the answer to this question is "yes," without a doubt. At a high level, security intelligence falls into three distinct categories, each with its own benefits:

1. **Open source security intelligence.** This category includes all publicly available security intelligence from security vendors, universities, researchers, security organizations, and government entities. While this intelligence is certainly valuable, various reports tend to be highly redundant with one another. Additionally, intelligence data tends to be *a posteriori* in nature. In other words, it is based upon knowledge acquired by experience such as known attack patterns, malware, and vulnerabilities.
2. **Product-based intelligence.** In this case, security intelligence is really an adjunct service that is tightly integrated with specific security technologies such as antivirus software, IDS/IPS, or web threat management. With product-based intelligence, security vendors use their install base as part of their research community. When a customer experiences a new type of attack, security vendors capture the event, develop a countermeasure, and distribute it throughout their customer base. Some vendors enhance product-based intelligence with their own research and some even productize their intelligence so they can offer it as an independent service. In general, product-based intelligence's link between intelligence and remediation is quite valuable, but it tends to be limited to a specific type of security technology or control.
3. **Independent security intelligence services.** This type of security intelligence is focused on the "dark side" of the Internet—malnets, cybercriminals, malware patterns, etc. Independent security intelligence includes basic services like reputation lists (IP reputation, website reputation) and deep analytics based upon mathematical algorithms that can apply a risk score to things like hosts, IP addresses, files, malware, etc. Enterprise organizations can then use these risk scores to help automate security policies. For example, security professionals can set up automated rules for blocking an external host when it receives a risk score in excess of 90 (out of a possible risk score of 100). Given the scale and scope of independent security intelligence, smart CISOs can utilize it to address a multitude of risks with proactive adjustments to security controls.

In reality, CISOs should really consume all three types of security intelligence, but it is realistic to expect different value from each one (see Table 2).

Table 2. Security Intelligence Description and Value

	Description	Value	Comment
Open source security intelligence	Free security intelligence provided by an assortment of organizations	Historical overview of threats, vulnerabilities, malware, suspect hosts, IP addresses, and content	Basic requirement for all enterprise organizations. May be lag time between discovery and publication
Product-based security intelligence	Security intelligence service adjunct to on-premises security technology products	Creates a hub-and-spoke network for detection and distribution of security intelligence	Improves security controls but may create security intelligence silos
Independent security intelligence services	Commercial threat intelligence services that are independent of any specific security products	Broad coverage of security intelligence focused on real-time discovery and distribution of new threat, vulnerability, malware, and suspicious threat actors	Can be integrated with various security controls to help automate risk management remediation and security operations

Source: Enterprise Strategy Group, 2014.

Introducing Norse

Enterprise CISOs recognize that they need help addressing cybersecurity complexity and the increasingly dangerous threat landscape. In fact, new cybersecurity requirements are driving a wave of product and service innovation. Good news overall, but many security professionals are growing progressively more confused by this avalanche of options. For example, which type of commercial security intelligence can help improve risk management and deliver strong ROI?

ESG recently met Norse, an innovative company focused on live threat intelligence, which may help illustrate how enterprise-class security intelligence services are evolving. What's interesting about Norse is that it has tailored its independent security intelligence services to the behavior and manifestations of the modern threat landscape, including cybercriminal rings, darknets, and network-based attack patterns. Norse can then analyze this data, separate out the noise, and provide true actionable intelligence to its customers.

Norse accomplishes this by:

- **Establishing a presence on the dark side.** Norse employs millions of physical and virtual distributed agents across the Internet backbone to gather live (i.e., real-time) security intelligence on network traffic. In this way, Norse observes traffic beyond customer sites and it can concentrate its monitoring and research efforts on the bad neighborhoods of the Internet: darknets, TOR networks, IRC channels, P2P networks, and Internet proxies where cybercriminals tend to congregate.
- **Baiting the bad guys.** Aside from passive network observation, Norse uses a number of surveillance tools like advanced honeypots and attractive "don't ask, don't tell" open source software services to actively engage hackers and study their behavior. This intelligence is used in concert with observable network activity to further pinpoint bad actors and truly malicious activities.
- **Doing the math.** Norse analyzes traffic patterns through algorithms composed of over 1,500 various risk factors. The result of this analysis includes Norse's IPQ risk scoring system based on a scale of zero (no risk) to 100 (extreme risk). These calculations are executed based upon Norse's massive data collection and big data security analytics performed in the cloud.
- **Addressing the cybersecurity skills shortage.** According to ESG research, 39% of surveyed enterprise organizations are challenged by a lack of skilled professionals in their security operations/incident response team.[2] These firms can't simply hire security professionals to bridge this gap given the global information

[2] Source: Ibid.

security skills shortage. What's needed here is security intelligence and security operations automation to help over-worked security teams work smarter; not harder. Norse does just this because its focus on cybercrime and hackers can help organizations increase the efficiency of security staff by streamlining investigations and automating remediation.

- **Providing actionable security intelligence.** Norse security intelligence can be viewed in numerous reports and threat feeds, but it can be used most effectively for security operations automation by integrating Norse risk scores directly with security controls like network firewalls, SIEM systems, and network access control points. Norse security intelligence enables this integration through a RESTful API for data exchange. In this way, CISOs can automate security operations by taking enforcement actions when Norse IPQ scores exceed a certain threshold.

Norse can also be a good investment for security intelligence around the emerging Internet of things (IoT) because its security intelligence platform is able to detect compromised, embedded, and connected devices and provide organizations with intelligence via API, identifying IP addresses of sensors and actuators that are malicious or high risk.

Given its scale, scope, and real-time intelligence feeds, Norse can be used for a number of high-priority security use cases including automating perimeter protection, providing cloud-based intelligence for fraud protection, and adding a layer of defense against advanced and targeted malware threats.

The Bigger Truth

As Albert Einstein once said, "The definition of insanity is doing the same thing over and over again and expecting different results." Regrettably, many CISOs are doing exactly that—believing that status quo and security controls can protect them against today's advanced threats.

Prevention is still important, but enterprise organizations must accept the fact that they will likely suffer security breaches in spite of all of their investments and efforts with security controls. This simply means that CISOs must bolster their capabilities around incident detection and response, and doing so must include better internal and external security intelligence as well as advanced security analytics. Armed with the right data at the right time, CISOs can then make better and timelier risk management, incident detection, and remediation decisions.

Moving forward, enterprise organizations must build an information security architecture capable of reacting to changes in the threat landscape as they occur. This type of design must be based upon timely security intelligence and security operations automation, helping to take the lag time and guesswork out of security decisions. Of course, advanced cybersecurity capabilities like these must be based upon real-time, accurate, and pertinent security intelligence as a foundation for security policy enforcement. Norse is one of a handful of independent security intelligence providers that is designing and building its services with this design for emerging enterprise security requirements.