ESG Brief

Webroot Delivers Enterprise-Class Threat Intelligence to Security Technology Providers and Large Organizations

Date: September 2014 **Author:** Jon Oltsik, Senior Principal Analyst; Kyle Prigmore, Research Associate

Abstract: *Large and well-funded enterprise organizations are struggling with incident detection and incident response, increasing risks associated with today's increasingly dangerous threat landscape. One way of addressing this situation is with the greater use of information-driven security based upon internal security analytics and external threat intelligence. ESG believes that the threat intelligence market will evolve as vendors correlate across multiple types of data types and add advanced analytics to deliver enterprise-class threat intelligence. Webroot is already establishing a leadership position in this market with its BrightCloud threat intelligence offering. With BrightCloud, Webroot can provide "wide-and-deep" threat intelligence directly to enterprise organizations or integrate threat intelligence with security prevention and detection technologies. When BrightCloud is integrated into security processes and infrastructure, it can help organizations streamline security operations with automated remediation, and enhance security investigations with correlated views of threat data.*

Overview

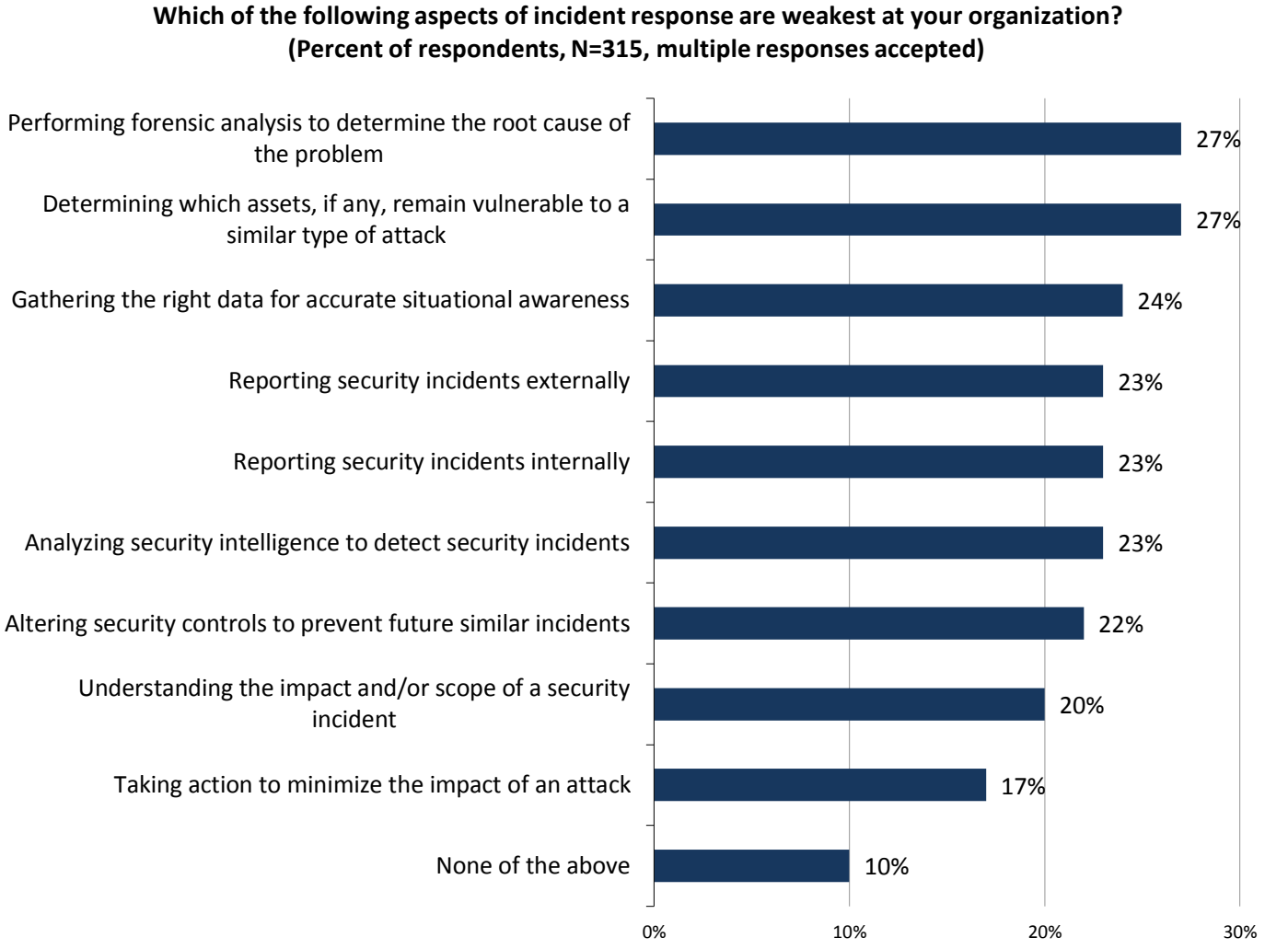
Enterprise CISOs are dealing with are being forced to deal with a few alarming facts:

1. The malware landscape is more perilous than ever before. According to ESG research, 49% of large organizations suffered a malware-based breach over the last two years. Even more alarming, 22% of enterprises claim that they've experienced more than 25 malware-based security breaches over the past two years.[1]
2. The global cybersecurity skills shortage makes it much more difficult to mitigate risk associated with malware threats. In fact, ESG research indicates that 25% of organizations claim that they have a "problematic shortage" of IT security skills.[2]
3. Many enterprises also have a multitude of incident detection and response challenges. ESG research shows that 27% of enterprises are relatively weak when it comes to performing forensic analysis to determine the root cause of a problem, 27% find it difficult to determine which assets may be vulnerable to a similar type of attack, and 24% have shortcomings with regard to gathering the right data for situational awareness (see Figure 1).[3]

One way of addressing this situation is with the greater use of information-driven security based upon internal security analytics and external threat intelligence. ESG believes that the threat intelligence market will evolve as vendors correlate across multiple types of data types and add advanced analytics to deliver enterprise-class threat intelligence.

[1] Source: ESG Research Report, *Advanced Malware Detection and Prevention Trends*, September 2013.
[2] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.
[3] Source: ESG Research Report, *Security Management and Operations*, July 2012.

Figure 1. Incident Detection/Response Weaknesses



Source: Enterprise Strategy Group, 2014.

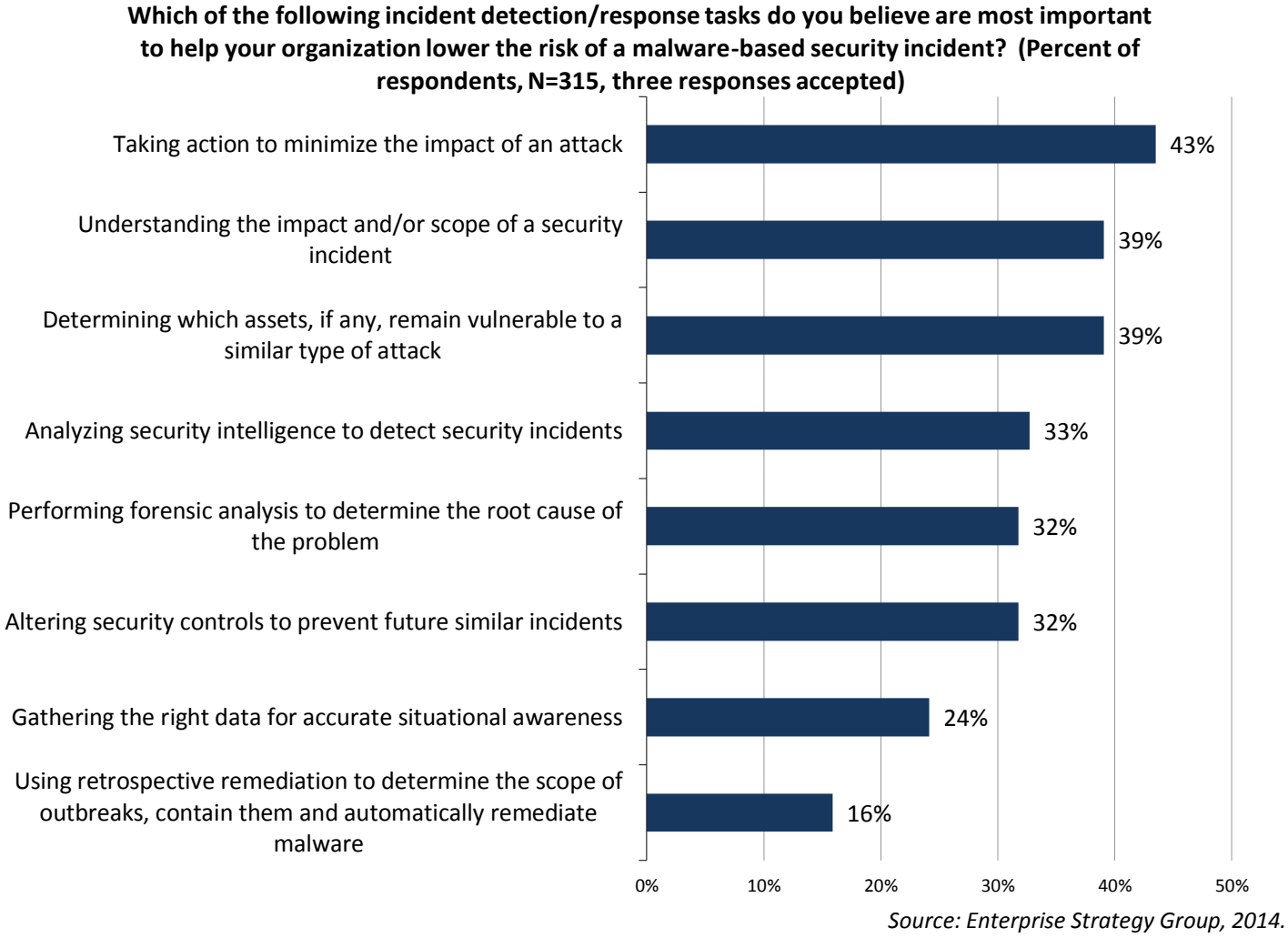
Enterprises are Turning to Information-Driven Security

Based upon the issues presented above, large organizations have to find ways to address the threat landscape and improve incident detection/response but they can't count on an army of new cybersecurity professionals to help them in these areas. In other words, CISOs have to employ the right people, processes, and technologies that enable their security teams to work smarter, not harder.

This critical realization is starting to have an impact on large organizations. To make better, smarter, and faster cybersecurity decisions, many firms are embracing information-driven security where organizations collect, process, and analyze large volumes of security data and then use this data analysis to guide their cybersecurity tactics—which activities to prioritize, which remediation tasks they pursue, how they conduct security investigations, etc. Information-driven security is an essential component to all of the most important activities identified by enterprise security professionals to help their organizations lower the risk of a malware-based security incident (see Figure 2).[4]

[4] Source: ESG Research Report, *Advanced Malware Detection and Protection Trends*, September 2013.

Figure 2. Most Important Incident Detection/Response Tasks



Source: Enterprise Strategy Group, 2014.

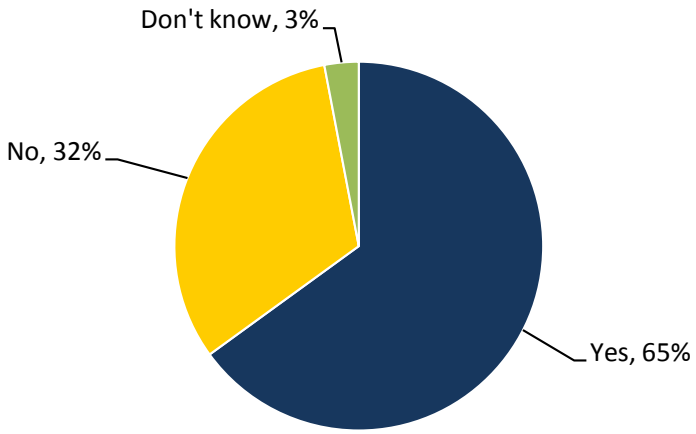
Threat Intelligence to the Rescue?

Information-driven security is initiating a new era in security analytics. In the past, many firms relied on internal log data and internal security alerts as the foundation of security analytics. Given the issues described above, however, large organizations are now collecting and analyzing a myriad of other data from sources like network packets, NetFlow, endpoint forensic, and profiling data, etc. Enterprises are also increasing consumption and utilization of external threat intelligence to gain a greater understanding of what's happening "in the wild." In fact, ESG research indicates that 65% of enterprises use external threat intelligence as part of their security analytics activities (see Figure 3).[5] Of those organizations that consume external threat intelligence, 94% say that it is highly effective or somewhat effective in helping them better address cybersecurity risk.

[5] Source: ESG Research Report, *The Emerging Intersection Between Big Data and Security Analytics*, November 2012.

Figure 3. Enterprise Use of Threat Intelligence

Does your organization use external threat intelligence as part of its information security analytics activities? (Percent of respondents, N=257)



Source: Enterprise Strategy Group, 2014.

In general terms, threat intelligence is offered in 3 ways:

1. **As "open source" feeds and reports.** Open source threat intelligence focused in areas like software vulnerabilities, IP reputation, SPAM and phishing sites, etc., is freely available and is thus a ubiquitous source for security analysts. This data is essential but is generally considered a baseline summary of discrete threats and vulnerabilities rather than a more comprehensive data set.
2. **As commercial threat intelligence feeds.** Many security vendors offer threat intelligence as a service. Threat intelligence in this category is more thorough than open source as vendors tend to add value with data correlation and analytics.
3. **Integrated into enterprise security technologies.** This trend has gained momentum over the past few years as the integration of external threat intelligence and enterprise security technologies can deliver a number of benefits. For example, network security devices can consume threat intelligence to automatically update rules for blocking malicious IP addresses, URLs, and files. Security analytics engines can use threat intelligence to identify suspicious behavior or network connections as part of security investigations. Advanced malware detection systems can use threat intelligence to calculate risk scores associated with suspicious files, or application binaries. These high-value use cases are driving threat intelligence integration into security technologies across the enterprise.

All Threat Intelligence is not Created Equally

While large organizations are consuming threat intelligence to improve risk management and incident detection/response, not all threat intelligence is created equally. In fact, most threat intelligence tends to be basic and redundant with narrow views on a single aspect of the threat landscape. These are often crowd-sourced data feeds that may contain out-of-date information and be prone to high rates of false positives. Alternatively, ESG believes that a new type of enterprise-class threat intelligence could be far more useful for security organizations or security technology integration. To maximize enterprise benefits, ESG believes that enterprise-class threat intelligence must be "wide-and-deep," including:

- **A wide assortment of data sources.** Rather than focus on one threat intelligence area or another, enterprise-class threat intelligence must offer a comprehensive view across a multitude of areas like IP reputation, URL reputation, file reputation, mobile app reputation, and real-time anti-phishing.
- **Massive quantities of data from all geographic locations.** Enterprise-class threat intelligence should include large data sets including billions of URLs and file behavior records across millions of domains, IP addresses, etc. This data must be collected, processed, analyzed, and then distributed to enterprises on a real-time basis.
- **Advanced algorithms and data correlation.** While data variety and volume is essential, enterprise-class threat intelligence vendors will really distinguish themselves by the way they apply big data security analytics to contextualize, correlate, and extract value from the data itself. The best threat intelligence will also be "actionable." In other words, specific threat intelligence will be timely and accurate, enabling forensic analysts and security technologies to have a high-degree of confidence in the data, and trigger immediate activities for risk mitigation, incident detection, or remediation.

Webroot BrightCloud for Enterprise Organizations and Security Technology Vendors

While many vendors are making bold claims, Webroot is actually delivering real enterprise-class threat intelligence with its BrightCloud service today. Unlike others, Webroot is offering a solution on both sides of the problem—a faster, simpler threat intelligence service for enterprise customers and a partnership program where security vendors integrate BrightCloud into prevention and detection technologies.

From a technology perspective, BrightCloud checks the applicable enterprise-class threat intelligence boxes. Its intelligence network is far-reaching, boasting some 8 million sensors that capture activities of 11 million mobile applications, 4.3 billion IP addresses (900 million of which have exhibited at least one security incident in the past and approximately 12 million deemed malicious at any given time), and 13 billion classified and scored URLs in their database (numbers which are raised by the millions per day and updated in real time). Webroot's threat intelligence network combines its internet sensors with information from its consumer and business endpoint customers, vetted global databases, and participating security partners to provide a broad security services offering to partners and customers. BrightCloud also collects, contextualizes, and correlates a wide range of data including web classification, web reputation, IP reputation, real time anti-phishing, file reputation, etc. With this breadth and depth, BrightCloud can help security analysts continually monitor resources, respond to threats, and update their policies from a central location. Alternatively, BrightCloud partners can integrate intelligence directly into on-premises security technologies to deliver accurate and timely threat intelligence for more efficient and automated threat prevention, detection, and response.

In addition to its current enterprise and partner offerings, ESG also believes that the BrightCloud roadmap should further strengthen Webroot's position with enterprise organizations and security technology OEMs in the future. For example:

- **Webroot plans to enhance BrightCloud's capabilities as a standalone product.** Webroot is intent on creating new algorithms to fine-tune its threat intelligence toward industry threats, geographic threats, targeted attacks, etc. Furthermore, Webroot recently launched solutions for large enterprises to directly incorporate threat intelligence into their security infrastructure through next generation firewalls and SIEMs.
- **Webroot OEMs bring a "network effect" to BrightCloud.** Webroot already has a large number of OEM partners including F5 Networks, Cisco Microsoft, Palo Alto Networks, and RSA Security. As participating OEMs can opt-in to share threat intelligence with Webroot, BrightCloud benefits from additional "eyes-and-ears" acting as sensors on the network. All BrightCloud OEMs gain as the self-learning BrightCloud network gets smarter over time.
- **Webroot is educating the market about the benefits of threat intelligence.** Many threat intelligence vendors have a cybersecurity research or academic focus, minimizing their value for enterprises facing high-dollar cybersecurity risk. Webroot maintains an enterprise perspective for using threat intelligence as a way to make day-to-day processes and tasks easier to manage. Future enhancements will continue this trend.

The Bigger Truth

The threat intelligence market is still in its infancy, and it is difficult to know at this point which vendors will win out over the long haul. However, ESG is fairly confident that based on its comprehensive enterprise-class offerings, Webroot is well-positioned to make an extended run at becoming a leader in threat intelligence for enterprises and a worthwhile partner for security technology companies. As such, CISOs should consider BrightCloud to improve risk management and incident detection/response, while security vendors look to Webroot to help them improve the efficacy and value of their prevention and detection technologies.