Achieving Continuous Intelligence with Advanced Security Analytics

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for SumoLogic

November 2015

EMA™

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

Information security has always been a large producer and consumer of data. More sophisticated best practices and expanding compliance and regulatory requirements have almost exponentially accelerated the production and consumption of data. Event and activity logs have grown to big data proportions and the diversity of data being consumed has become significantly more varied. As the need for continuous security intelligence and accelerated incident response increases, traditional log and event management tools and monitoring practices are becoming increasingly insufficient.

IT and security are deluged with thousands of alerts daily—a majority of which appear to be critical—making response an insurmountable task with affordable staff levels and traditional tools. With so many critical alerts, IT and security have moved from the analogy of finding the needle in the haystack, to identifying and prioritizing the needle in the stack of needles.

The era of big data is demonstrating to information security that there is more that can and must be done to identify threats, reduce risk, address fraud, and improve compliance monitoring activities by bringing better context to data and creating information for actionable intelligence.

This research studies how both management- and operations-level IT and information security practitioners perceive the change in the volume and types of data available and the tools needed to provide analysis to generate actionable threat intelligence.

Advanced security analytics provides new adaptive algorithms called machine learning as well as big data analysis techniques that can be utilized to identify abstract data relationships, anomalies, trends, and fraudulent and other behavioral patterns, creating information where only data existed. The era of big data is driving the next technology evolution.

Security analytics, though a relatively new field of technology, is the next step in the areas of detection and response, with possible impacts on prevention as well. Machine-learning algorithms and analysis techniques have advanced far beyond the capabilities of what was available in the commercial markets only two to three years ago. They also address the issue dubbed "We don't know what we don't know." Security analytics' core function is to monitor and collect vast amounts of information from the environment to identify threats that indicate elevated risk and ultimately prevent lateral spread of those threats and data exfiltration. To succeed in this endeavor, the analytics platform performs the identification of threats and prioritization of threats without the requirement for the administrators and analysts to create policies or rules.

Security analytics tools provide practitioners a means to meet their needs for continuous actionable security intelligence to provide timely response to attacks and prevent attacks from becoming breaches.

Security Data Is Unmanageable with Legacy SIEM Tools

In the recent research report *Data-driven Security Reloaded* (DDSR), Enterprise Management Associates® (EMA™) asked over 200 security, fraud, risk, and IT professionals what their top five use cases were for security technology. By order of precedence, the responses were as follows.

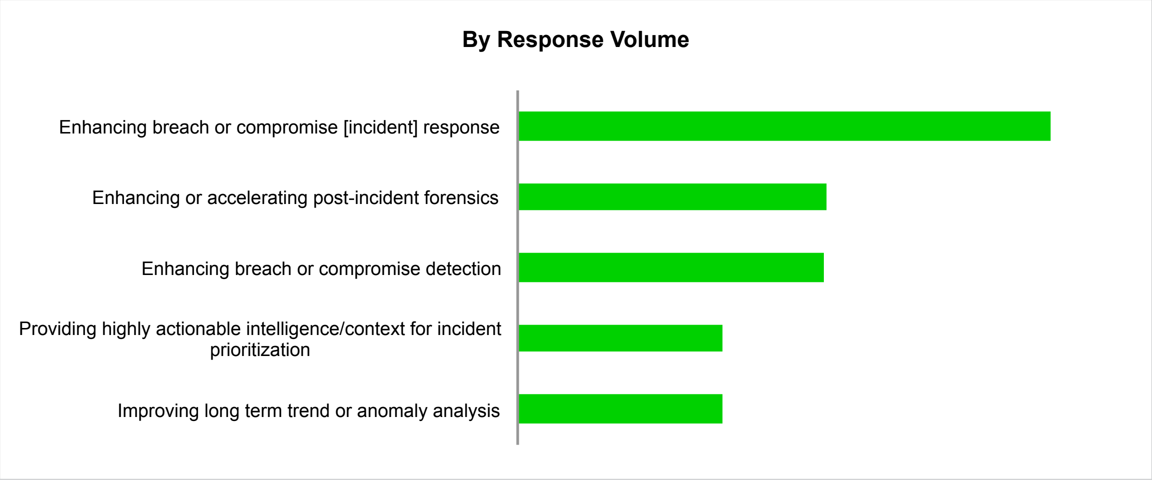

Figure 1. Top 5 Use Cases for Security Technology

These use cases drive a set of data analysis requirements far beyond what most organizations are capable of delivering with a traditional SIEM or log management tool. Traditional SIEM and log management tools rely on thresholds, policies, triggers, and rules created by the operators and administrators to alert analysts of potential problems. The two primary problems with this methodology are first, the need to know what you are looking for to create the context for the alert, and second, as data ebbs and flows, many times the alerting rules are too tight or too loose. When alerting rules are too tight, it means that they are regularly exceeded, and too many false alerts are created. When alerting rules are loose, it means they do not alert on a problem because the alerting requirements have not been met. This is a common scenario for many organizations and one that is difficult to solve without changing the mentality from alerting to analysis.

Having to know what attack signals to look for in order to be made aware of issues has the same flaws as signature-based malware detection. It can look for known threats, but it cannot find zero-day, advanced targeted attacks (ATA) and advanced persistent threats (APT).

Successful Security Means Bringing Data Silos Together to Provide Continuous, Hi-fidelity, and Actionable Intelligence

All organizations have capabilities gaps in their security programs. As would be expected, the gaps vary considerably based on industry vertical, organization size, revenue, and other factors. When the DDSR research drilled down into how organizations were looking to remedy these gaps over the next one to three years, 51% of the participants said they were looking to IT security technologies and their vendors to lead the way. This was the greatest single response for this issue. It made it clear that, though not all gaps are technology-related, respondents believe most of the issues need better technology and it is up to solutions providers to create it.

DDSR respondents were asked about their top five frustration points with the security programs capabilities. Forty percent of participants said their single highest frustration was "The lack of integration/interoperability among vendor solutions." The second most common answer with 38% was "Tools are unable to recognize new and emerging threats." Participants were also asked what their top five dissatisfiers were with the technology they already had in place. Just over 50% of respondents said "Too many false positives." The other four top issues with technology were "Inadequate ability for correlating security incidents to business impact," "Inadequate staff or expertise to get the necessary ROI out of current tools," "The technology can't handle the volume of data collected," and lastly, "Inadequate visibility into threats ingress and or propagation in the environment."

The DDSR research project was designed to determine if participants believed or knew of technology that would solve these problems. Of the 18 categories of technology included in the report, only one seemed to offer the possibility of solving these issues in a single package. That solution was advanced security analytics and anomaly detection. According to respondents using security analytics, it provided them the highest value as related to total cost of ownership (TCO) out of all of the 18 categories.

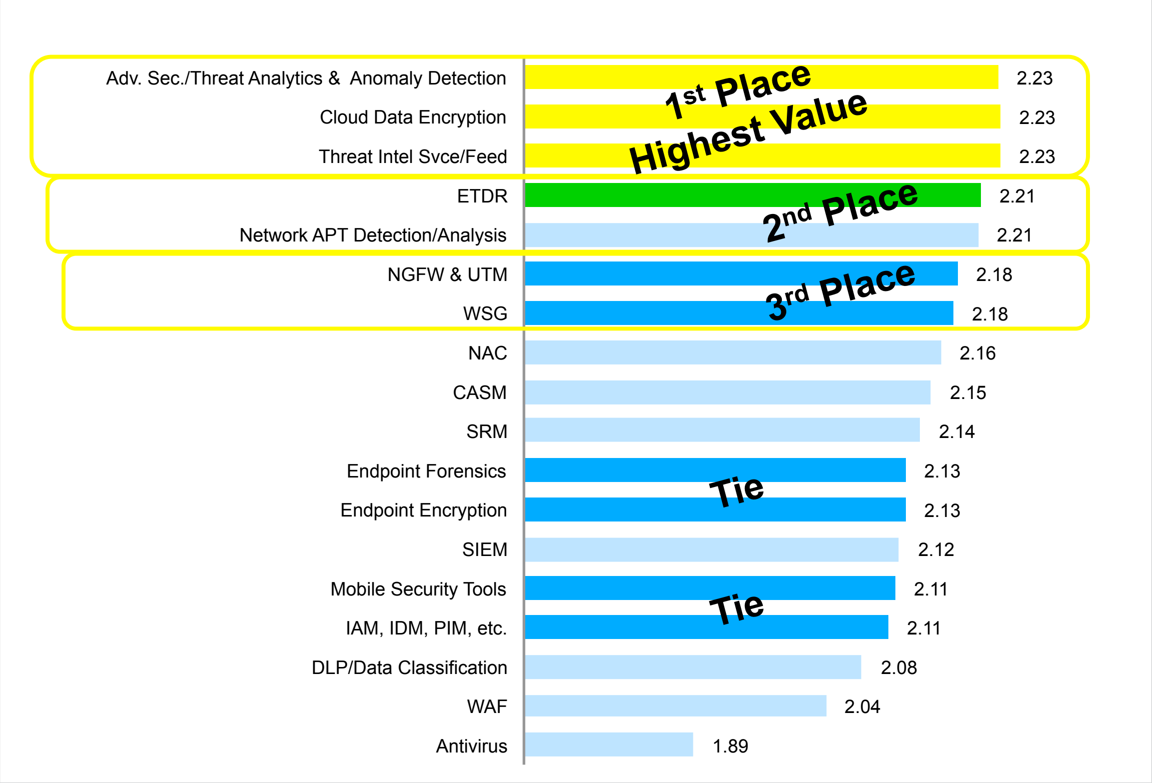

Figure 2. Mean Perceived Value of Technologies Based on TCO

Security analytics, also sometimes referred to as security intelligence and threat analytics, is a relatively new area of technology created to close the gap where prevention and other forms of detection fail. Its primary purpose is to accelerate detection and incident response by providing earlier visibility into activities within the target environment that could indicate compromise or any variety of malicious activities which may negatively impact the organization. When effectively deployed, it provides early warning of those activities to stop lateral movement of the threat and prevent data exfiltration and other destructive events.

Security analytics generally takes one of three forms: anomaly detection, user behavior analytics, and predictive analytics. To deliver on the objectives of increased detection and accelerated response and containment, security analytics may create its own source data and metadata. It may also aggregate data through various types of collections, which can include both structured and unstructured data ranging from entity (application, system, or user) activity logs, to packet stream and protocol interrogation, and even to sandbox execution of code. It may also ingest data from other log sources and interface with other monitoring and alerting systems, like security incident and event management systems (SIEM). This produces the highest fidelity intelligence for rendering the context of an event, which creates the highest level of visibility possible into activities in the environment, ultimately rendering the best prioritization of incidents for responders to address.

SIEM is *Not* Security Analytics

Security incident and event management or SIEM tools were also in the DDSR report, but they did not fare as well. SIEM has become a mainstay of many midsized and large enterprises. It is a workhorse that is able to collect, receive, process, normalize, correlate, and alert on issues within the environment. However, traditional SIEM is not intelligent. It has little to no true internal analysis capabilities. With all it can do, SIEM is limited to identifying the issues for which it has created rules, policies, triggers, and/or thresholds. The administrators and operators have to know what they are looking for and then have the ability to create the context for the alerts they wish to receive. This limitation causes SIEM to deliver anywhere from hundreds to thousands of critical alerts, overwhelming operations and analyst teams. On the other side of the issue, when contexts are tuned to reduce alert volumes, many real indicators of attack and compromise do not create alerts, which increases risks to the organization. This particular scenario has been relived multiple times in the last year alone, leading to successful attacks on organizations like Sony, Target, and Home Depot.

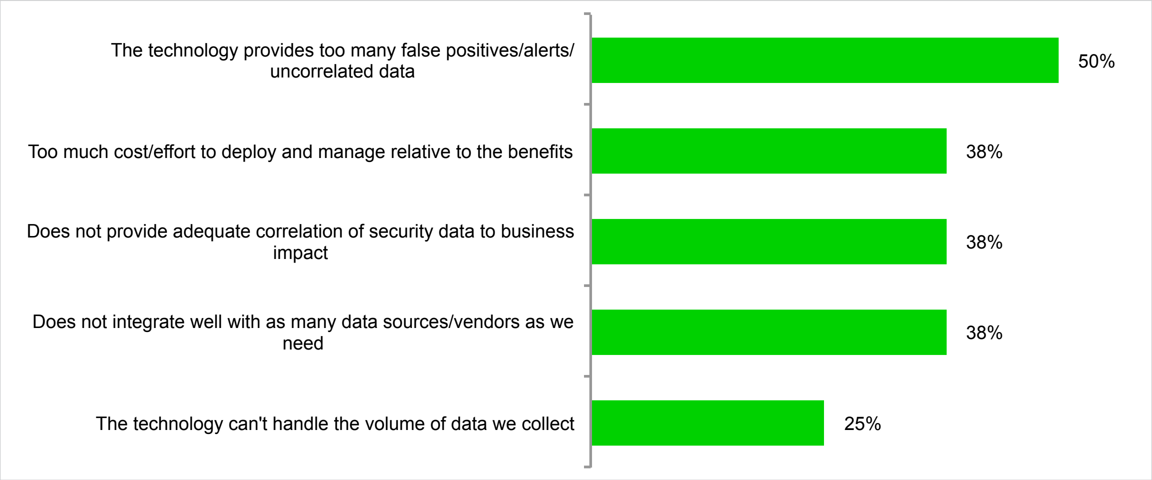

Figure 3. Top 5 Dissatisfiers with SIEM Technology

In the DDSR research, 46% of respondents believed that security analytics is the next evolution in SIEM technology. To deliver on its promises of increased detection, accelerated response, and containment, security analytics has an internal "analysis" capability. Whether using its own source data and metadata, or aggregated data from existing monitoring systems, security analytics adds decision-making value from its analysis capability, which SIEM technology does not provide.

Ultimately, 100% of organizations that deployed only security analytics experienced a reduction in false alerts or improved actionable alerts, while only 60% of organizations that deployed SIEM said they experienced improvements.

Security Analytics Separate the "Normal" from "Abnormal" Activities

Security analytics uses many forms of advanced analysis, including statistical deviation, Bayesian analytics, and probability analysis. It also provides a new class of adaptive algorithms classified as "unassisted machine learning" to identify and alert on activities in the environment which are abnormal and should be investigated.

In DDSR, 33% of the respondents indicated that one of their top five most significant frustrations with their IT security capabilities was "Too difficult to distinguish normal from abnormal activity." Machine-learning algorithms learn from, not only individual entity behaviors, but also from group behaviors to quickly adapt to the environment, thus removing the previous requirements of other technology to require either a clean sample at start or a long learning time in order to produce accurate alerting. This adaptability creates the context for actionable alerts, which address a second frustration with IT security capabilities that SIEM has not. Thirty-three percent of respondents said it was "Too difficult to prioritize remediation of threats" in their environment. With its toolset, security analytics provides better intelligence and adaptability, which lead to a better ability to stop threats.

To further understand gaps and issues in security, DDSR asked respondents what they believe are the top three most needed improvements for information security as a discipline. This question has been asked all three years the *Data-driven Security* report series has been run, and it has uncovered a disturbing trend. The top three concerns have remained the same for each of the three years, and the percentage of respondents identifying them as concerns has been increasing each year. There is also a considerable increase in respondents identifying these issues between 2014 and 2015. The volume and diversity of breaches across the world increase the understanding that programmatic gaps are more than just troublesome—better tooling is needed to fend off the onslaught. The figure below depicts the details on the issues and the trend.

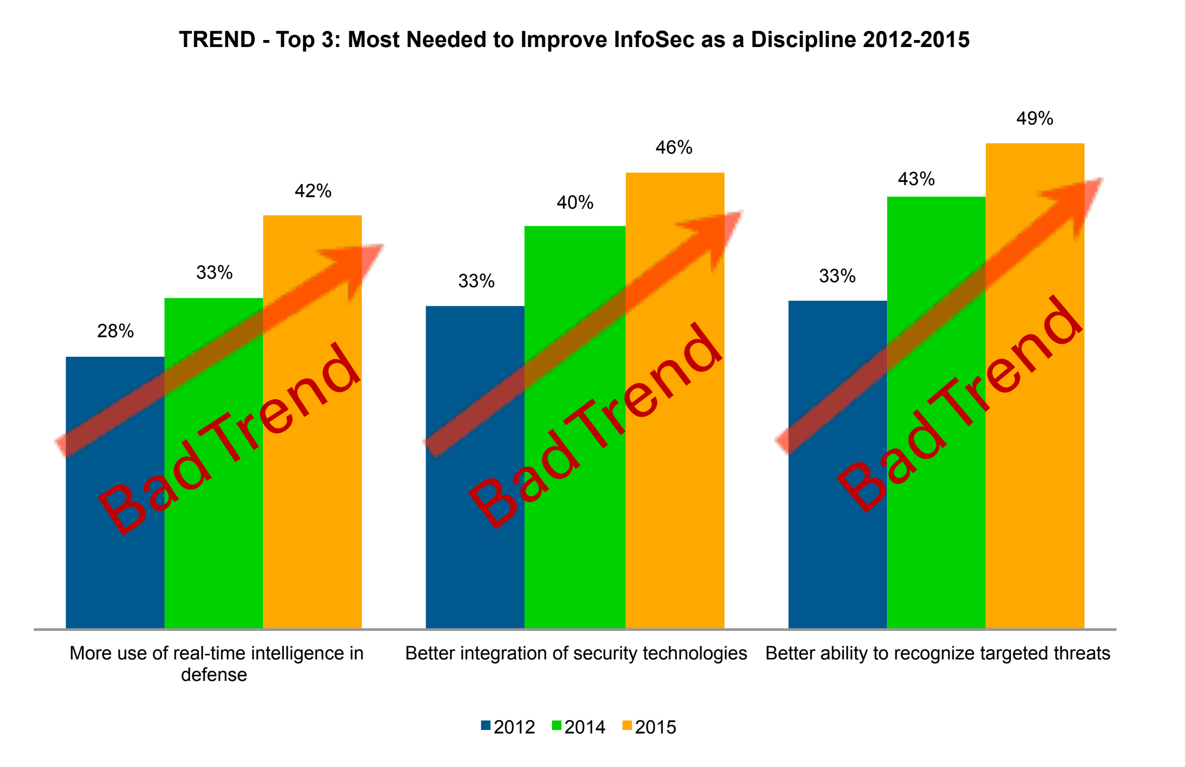

Figure 4. Does Security Know What It Doesn't Know?

In addition to these concerns, 79% of participants said that they were between only "somewhat confident and "highly doubtful" that their organization could detect a security issue before it presented significant impact to them. Respondents whose organizations had security analytics in place had significantly more confidence in their ability to detect and deal with all of these issues and were less threatened by them.

Over the three iterations of the *Data-driven Security* report series, EMA has seen a decline in respondents' ability to identify and monitor threats to high-risk assets and prioritize their response based on potential impacts on their organization. Most significantly, between 2014 and 2015, the percentage of respondents dropped from 57 to 42%. This was a key tipping point in that now less than half of organizations are able to effectively protect their high value assets.

EMA Perspective

The issues security organizations face today create both a significant problem and excellent opportunity for solutions providers. Budgets, attacks, and breaches are up, but patience is waning. For the incumbent technology providers, there is a prospect of revenue loss from being displaced by newer technology or technologies that can relieve the frustrations with identifying indicators of malicious activities and compromise earlier in the attack cycle.

Following are what EMA sees as the core features needed for a security analytics vendor.

- Identify breaches early enough to stop threat propagation and data loss or exfiltration.
- Reduce the false positive rate to a significantly smaller number of actionable alerts.
- Provide reporting capabilities that identify risk and show business stakeholder value.
- Deliver automation and other continuous capabilities that are a force multiplier and reduce the need for human capital.
- Architect elastically to scale to meet both spikes in demand and growth over time.

✓ SumoLogic provides advanced security analytics through user behavior modeling, anomaly detection, and predictive analytics to ward off impending threats by uncovering unknown security issues without relying on rules or predefined schemas.

✓ SumoLogic ingestion is data agnostic, allowing its intelligence to create hi-fidelity actionable alerts.

✓ The customizable dashboards and reporting allow drill down to correlated events and individual events and can satisfy the informational needs of both security operations and businesses.

✓ SumoLogic removes the need to invest in hardware and manpower to operate the infrastructure so money can be spent finding and resolving security issues rather than operational and performance issues.

✓ SumoLogic technology was born in the cloud, so it scales to meet the performance needs of even the largest enterprises.

No technology should be considered a silver bullet. Each has its strengths and can provide value for some specific set of use cases. Security analytics needs data to do its job, so in many cases it relies on a solid logging and alerting infrastructure. However, given the proper data feed, it has proven itself to be a huge asset in solving numerous use cases. DDSR participants using security analytics were asked their top five reasons for needing the technology; these responses are shown below.

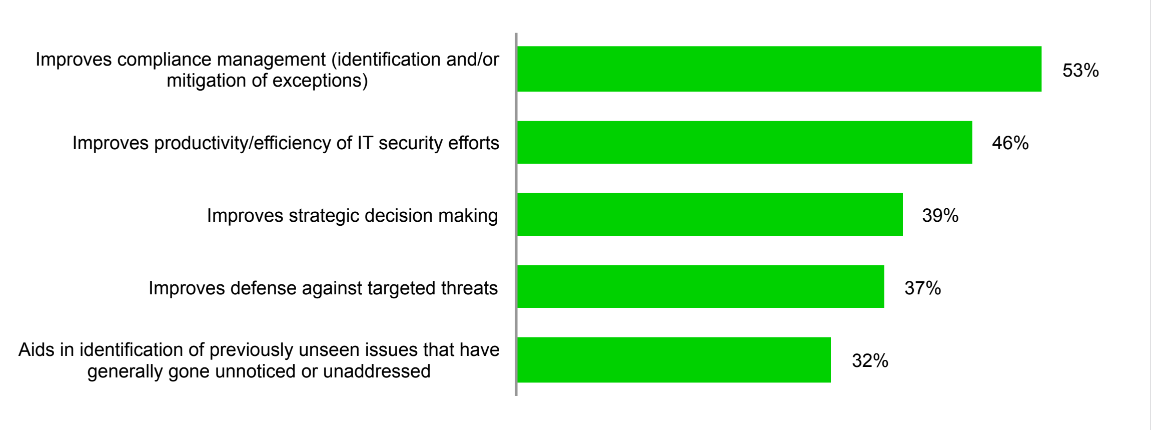

Figure 5. Top 5 Reasons Why Security Analytics Is Needed

Not only did security analytics improve compliance management, which is a strong driver in many organizations, but it is obvious that it addresses the strong need for increasing security operations efficiency in identifying and addressing threats via their indicators of compromise (IoC).

About SumoLogic

SumoLogic is the industry's secure, cloud-native, data analytics service, delivering real-time, continuous intelligence across an organization's entire infrastructure and application stack. More than 700 customers around the globe experience real-time operational, business and customer insights using SumoLogic for their DevOps, ITOps, and security and compliance use cases. With SumoLogic, customers gain a service model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value, and growth.

Founded in 2010, SumoLogic is a privately held company based in Redwood City, CA and is backed by Greylock Partners, Sutter Hill Ventures, Accel Partners, and Sequoia Capital. For more information, visit www.sumologic.com

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3272.110215