EMA Research Report: Data-Driven Security Reloaded

Summary of Research Findings

By David Monahan
An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report

April 2015

Research sponsored by:

prelert®

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 a result, traditional log and event management tools and monitoring practices are becoming increasingly insufficient.

To add to this, the success record of maintaining security for an environment is at an all-time low. Executives are being dismissed or forced to resign post breach whether they knew about security issues prior to the breach or not. Threats seem to come from every angle. Not only are attackers consistently probing, but the attacks themselves are more persistent and difficult to block; once a foothold is achieved, detection and removal are also more difficult.

This research summary discusses how both management- and operations-level IT and information security practitioners are impacted by staffing shortages, lack of visibility into their environments, and how they are getting higher fidelity data to provide better context for detection and response to incidents in a world where prevention has often failed. Security analytics tools provide practitioners with a way to meet their actionable threat intelligence needs for an appropriately prioritized, timely response to attacks. **Prelert**™ and **Enterprise Management Associates**® have partnered to provide this research, which identified that across the board, 79% of respondents were only "somewhat confident" in to "highly doubtful" of their ability to detect an important security issue before it had significant impact. In contrast, 95% of the participants using security analytics were between "highly confident" in and "somewhat confident" in their ability to detect similar issues, thus demonstrating that the information security discipline needs next generation analytics capabilities to be successful in the age of advanced and persistent threats.

95% of the participants using security analytics were between "highly confident" in and "somewhat confident" in their ability to detect an important security issue before it had significant impact.

Introduction

The Data-Driven Security Reloaded (DDSR) research survey studied 18 areas of technology in use by organizations to understand what technologies they are deploying, why they felt they did or did not receive value out of those technologies, and how they are using those technologies to prevent, detect, and respond to threats against their assets, especially information assets. Participants consisted of over 200 random respondents, including IT administrators supporting the security function and information security professionals and IT management supporting security. A representative cross section of industry verticals, including banking and finance, health care and pharmaceuticals, government, and manufacturing, were included with company sizes ranging from small to medium businesses to large enterprises. This report represents a summary of the findings from the research. The full report and corresponding summary report will be released in May 2015.

Information security has seen significant evolution in both landscape and threats in the last 25 years. The latest wave brings nation states battling for cyberspace dominance with ingenious and never-before-seen (zero-day) attacks. To make things worse, we are experiencing a similarly unprecedented

and rampant spread of international organized crime syndicates that leverage the new techniques they glean from nation states' activities, as well as some of their own tricks, to target personnel and systems to extract information in unparalleled quantities and with previously unseen persistence. To complete the trifecta, security is also experiencing the leading edge of the Internet of Things (IoT), which is the beginning of billions of unregulated and unmanaged devices that will make mobile smartphones look almost trivial in terms of security risk.

Security analytics provide advanced analysis algorithms, including a class of adaptive outcome algorithms called machine learning, to provide individual and community behavioral analysis combined with protocol, packet stream, and big data interrogation and risk profiling techniques to identify, prioritize, and contain both human- and malware-based threat actors.

The next few pages will set the stage and provide insights into IT and information security practitioners' perceptions of the need for advanced analytics and the evolution of data-driven security.

Setting the Foundation

What Is Security Analytics?

Before diving into the core report findings, it is important to create a common context or understanding of what security analytics is. Security analytics is a relatively new area of technology created to close the gap where prevention fails. Its primary purpose is to provide visibility into activities within the target environment that are indicators of compromise, thus accelerating incident response. When effectively deployed, it can provide an early enough warning of those activities to stop lateral movement of the threat and prevent data exfiltration.

What Does Security Analytics Do?

To deliver on the objectives of increased detection and accelerated response and containment, security analytics does not just create its own source data through various types of collection, which can include sandbox execution of code, packet stream and protocol interrogation, content interrogation, and activity anomaly detection. 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 both acquires the highest level of visibility possible into activities in the environment and produces the highest fidelity intelligence for rendering the context of an event, thus providing as few false positives as possible. This ultimately renders the best prioritization of incidents for responders to address.

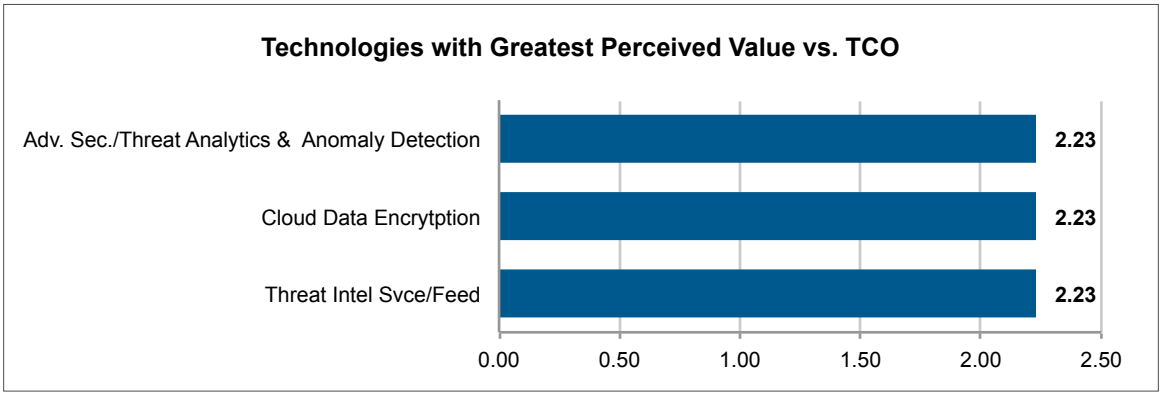
Each vendor platform has its own intellectual property and proprietary approach that, when combined, creates a unique solution, making it imperative for each organization to understand their requirements and discuss them with prospective vendors prior to purchasing a solution of this type.

Findings for Security Analytics

How Does It Benefit Organizations that Have It?

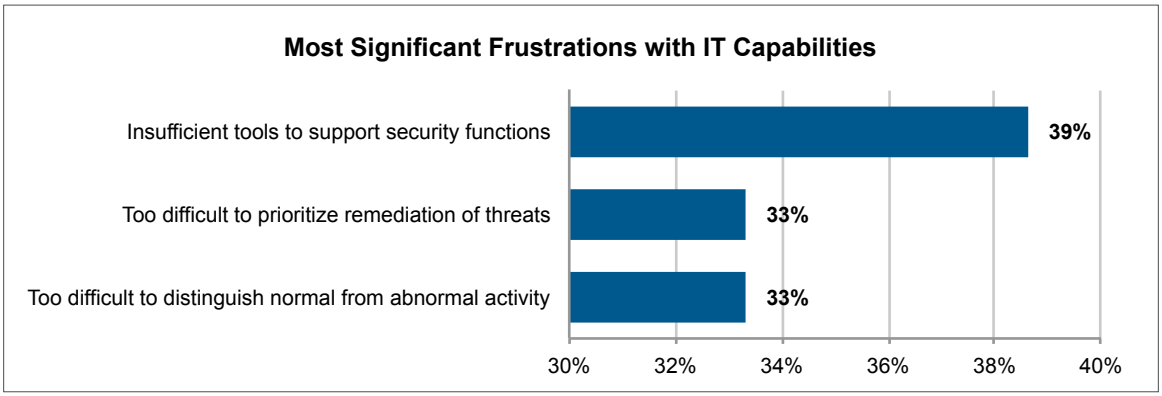
Though security analytics ranked second to last in deployment saturation among respondents, for the second year in a row it scored in the top ranking for perceived value when compared to total cost of ownership (TCO). Out of 18 evaluated technologies, it received a 2.23/3.00 for satisfaction, tying with cloud data encryption and threat intelligence services/feeds.

For the second year in a row security analytics scored in the top ranking for perceived value when compared to total cost of ownership (TCO).



An interesting note is that only 1% of security analytics owners expressed less than expected value vs. 6% for both threat intelligence and cloud encryption feeds, indicating that shortcomings were more from a failure on the customers part to properly determine requirements prior to purchase rather than a technology failing.

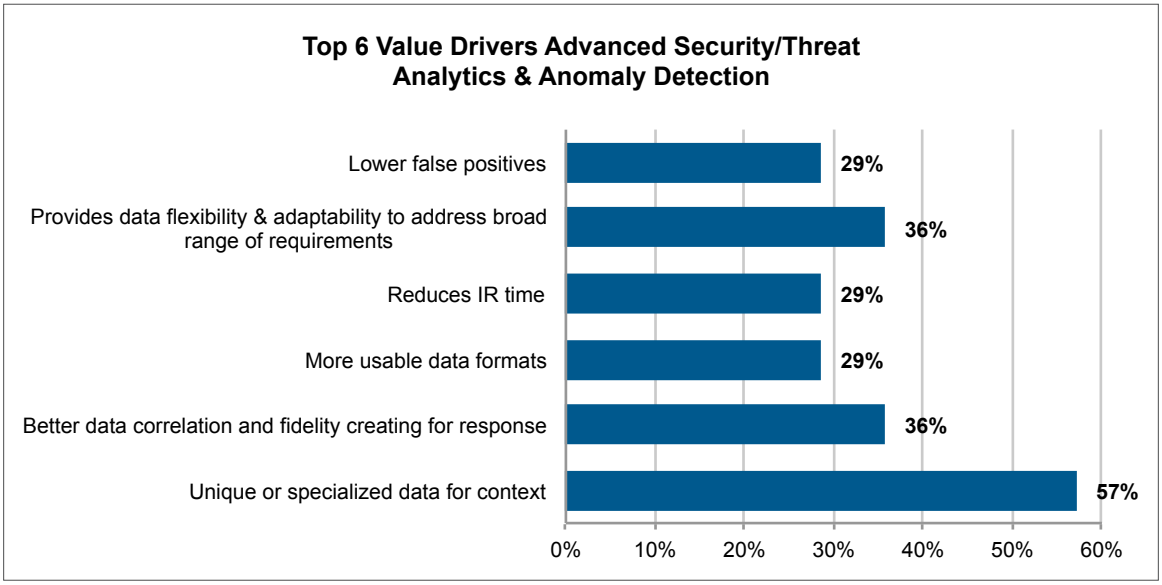
Security analytics solve a number of common problems in detecting and responding to threats. When asked about their top three most significant frustrations with IT capabilities, EMA received the following technology issues.



The first item can be interpreted as either a lack of tools caused by inadequate funding or a lack of ability to locate the proper tools. Security analytics can address the latter, as discussed in this report and more so in the full report, but the former is a management issue out of scope for this summary. Security analytics as a class of tool is designed from the ground up to address the prioritization of alerts

and identify the abnormal activities within the environment. In fact, respondents who had security analytics deployed emphasized other issues in this question such as lack of repeatable processes and personnel issues.

In correlation, when asked what their primary value drivers were for purchasing security analytics, participants provided the following feedback.



This demonstrates that security analytics provides a broad range of valuable services to the organization.

Security analytics also automates many of the tasks that a trained analyst would normally do, thus relieving them of time consuming tasks such as investigating alerts to check them as false positives, prioritizing them, and collecting artifacts to support response recommendations or activities. In fact, when asked about the use cases driving the need for security analytics, the top responses were the following.

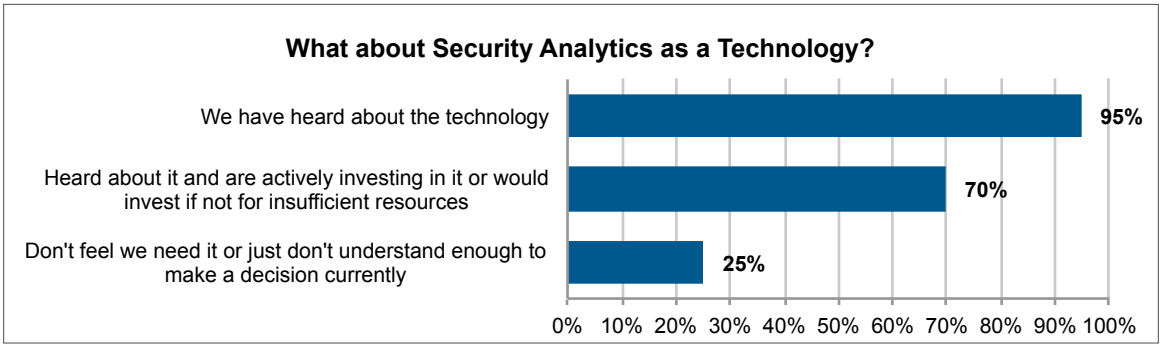
1. Providing highly actionable intelligence/context for incident prioritization
2. Providing data aggregation and correlation
3. Improving long-term trend or anomaly analysis
4. Enhancing or accelerating post-incident forensics
5. Enhancing breach or compromise [incident] response

When asked about their primary value drivers, 57% said security analytics "provided unique or specialized data for context," which is direly needed to identify today's stealthy threats.

When evaluated singularly, each of these use cases can be seen as valuable in its own right, but when viewed collectively, their capability to provide a significant force multiplier for an already taxed security organization is tremendous.

Summary

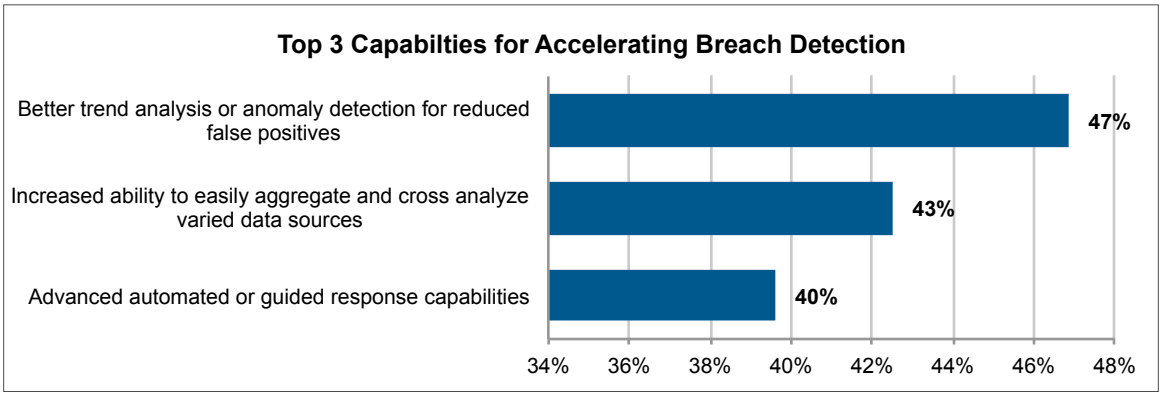
Security analytics, though a relatively new field of technology, is the next step in detection and response technology. Machine-learning algorithms and analysis techniques have advanced far beyond the capabilities of what was available in the commercial markets only 2-3 years ago. They also address the issue dubbed, "We don't know what we don't know." Security analytics' core function is to monitor and collect 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.



Only 25% of research participants respondents felt they did not need security analytics or just had not gotten educated enough to make a decision either way. This minority is less than last year, indicating that security analytics is making a strong entrance into the market space. After only a few years, 95% of research respondents said they are aware of the technology and 70% of participants indicated they either have an investment in the technology or would have an investment if it were not for insufficient resources at the time of survey.

When asked about their top three desired capabilities for accelerating breach detection, research participants identified these capabilities at the top of their list, all of which are provided by security analytics solutions.

Security analytics combines multiple capabilities for detection and response, each of which are significant strengths and are also not found in combination elsewhere in the technology market.



Security analytics combines multiple capabilities for detection and response, each of which are significant strengths and are also not found in combination elsewhere in the technology market.

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 its 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

3133_Prelert-Summary.041415