ESG Solution Showcase

An Analytics-based Approach to Cybersecurity

Date: May 2015 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: Since the Google Aurora incident announced in 2010, large organizations have faced a steady stream of APTs and targeted cyber-attacks. In some cases, these attacks have led to costly data breaches at organizations like Anthem, Inc., JPMorgan Chase, Sony Pictures, and Target. Why does this continue to happen? Unfortunately, many organizations are simply unprepared and lack the right cybersecurity strategies, skills, processes, and technologies. Enterprise organizations must come to grips with the new cybersecurity realities and requirements by altering their philosophies and embracing an early detection and rapid response and coordination strategy. To make this transition, CISOs must incorporate and provide analytics strategies and toolsets within their organizations as soon as possible.

Overview

Consider the following data breaches:

- Anthem, Inc., February 2015. The company announced that it had discovered a "very sophisticated external cyber-attack," which resulted in the theft of the personal information (i.e., medical ID numbers, social security numbers, income information, e-mail addresses, etc.) of 80 million customers/subscribers.
- US Postal Service, November 2014. Late last year, the USPS released information indicating that it suffered a data breach compromising the personal information of over 800,000 employees.
- Staples, Inc., October 2014. US-based office supply company Staples revealed that hackers used malware that provided access to transactional information at 115 stores. Nearly 1.2 million customer payment cards were exposed.
- Oregon Employment Department, October 2014. WorkSource Oregon discovered a data breach that provided unauthorized access to a database of individuals searching for jobs. The social security numbers of more than 850,000 individuals were compromised.

All told, these four data breaches occurred over the course of just five months and compromised the personal data of over 82 million people—almost a quarter of the US population! Also, there were an additional 87 data breaches during the same timeframe at a variety of other organizations, including Snapsaved, Sony Pictures, and the Texas Health and Human Services Department.

Why do organizations continue to experience so many cyber-attacks and data breaches? Over the past few years, cyber-adversaries have adopted the advanced persistent threat (APT) model as part of attack campaigns. This means they are

This ESG Solution Showcase was commissioned by Splunk and is distributed under license from ESG.
© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

willing to put time and resources into researching their targets, gaining valuable reconnaissance intelligence, pursuing multiple attack techniques along different vectors to gain trusted access to their targets, and then maintaining persistence to accomplish their objectives (the Lockheed Martin Cyber Kill Chain lifecycle). In other words, cyber-adversaries are willing to remain doggedly tenacious until they finally penetrate corporate networks, compromise systems, and complete their missions.

Enterprises Remain Unprepared

In the past, large organizations invested the bulk of their security resources in threat prevention processes and technologies. This focused on the first few steps of the attack lifecycle—preventing (blocking) the attack from delivering the malware and gaining access to a system. It also involved deploying systems in hardened configurations, installing antivirus software on endpoints and servers, patching software vulnerabilities, and blocking malicious IP addresses and URLs.

This approach and the associated processes/technologies were probably adequate for a singular component or automated threats like e-mail viruses, Internet worms, and spyware, but do not take into account the multiple steps associated with modern APTs and advanced attacks. Yes, strong security controls are still important, but organizations must now assume that attackers will circumvent defenses, penetrate networks, compromise systems, and advance their attacks.

Given this, large organizations must supplement attack prevention with a more thorough strategy for threat detection and incident response. This entails getting insight into all activities across networks, hosts (e.g., endpoints and servers), applications, and databases. It also includes monitoring, alerting, analyzing for incidents, and then coordinating, containing, remediating, and sharing threat intelligence as incorporated learnings back into the monitoring, alerting, and response process. Security teams also need the ability to identify attack activities using breadcrumbs of evidence found lying across the entire technology stack (e.g., firewalls, IPS, antivirus, and servers).

Unfortunately, threat detection, investigation, and response at many organizations remain relatively immature and manually intensive. ESG recently asked survey respondents to define their organization's biggest incident detection/response weaknesses, and the top three most-cited responses relate to situations where an attacker has gained access to the enterprise. From those responses, 29% of enterprise security professionals say they have an organizational weakness when performing forensic analysis to determine the root cause of a problem; 28% point to weaknesses using retrospective remediation to determine the scope of outbreaks, contain them, and remediate malware; and 27% say they are weak when it comes to analyzing security intelligence to detect security incidents (see Figure 1).[1]

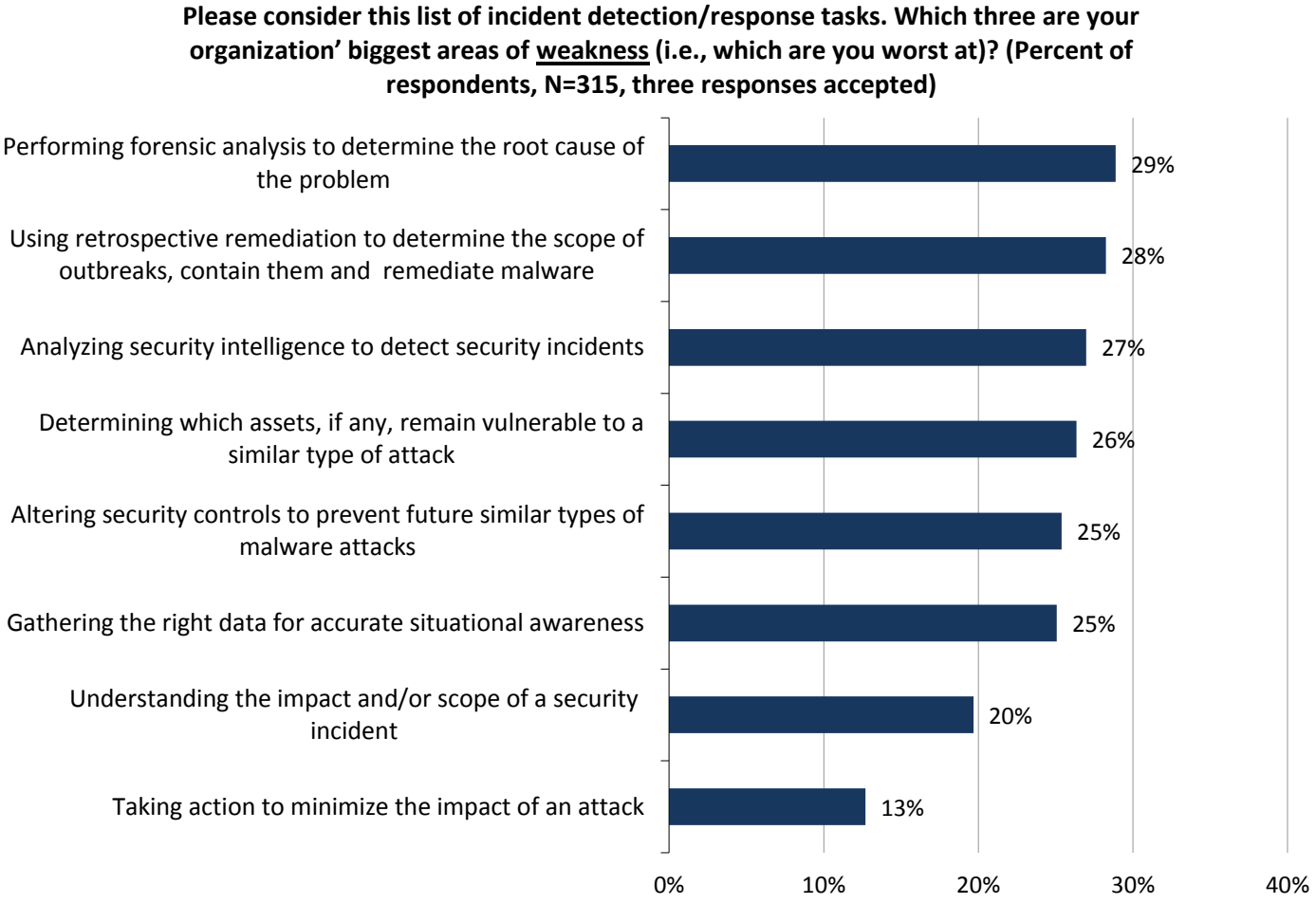
Rounding out the top most-cited five, the next two responses focused on avoiding a repeat attack of the same tactics: 26% report a weakness associated with determining which assets are vulnerable to similar attacks, and 25% remain weak with regard to altering security controls to prevent a similar attack.

The universal problem is how to quickly determine the root cause of incidents and then contain and remediate them. Once this is completed, the goal is to return intelligence from the analysis back into the system for continuous cybersecurity improvement.

[1] Source: ESG Research Report, *Advanced Malware Detection and Prevention*, September 2013.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

FIGURE 1. Incident Detection/Response Weaknesses



Source: Enterprise Strategy Group, 2015.

What about SIEM?

Many security professionals will look at this ESG research and insist that they have these weaknesses covered with their existing security information and event management (SIEM) platform. Since SIEM is designed to collect and correlate security events, logs, and network flow data for security analysis and operations, it's understandable that security professionals make this assumption.

So what's the problem? SIEM limitations can get in the way of addressing security requirements: According to previously conducted ESG research, enterprise security professionals have numerous problems with SIEMs related to the incident detection, analysis, and response (see Figure 2).[2] Security professionals struggle with SIEMs for the following reasons:

- **Event correlation is based on normalizing data relative to predefined schemas.** SIEM systems were originally designed to collect, filter, and correlate log events from security devices to identify issues from all the logs and alerts generated. By correlating the logs (seeing multiple events simultaneously that, when combined, are indicative of an issue), the SIEM could identify the most important alert(s) to investigate. In order to correlate events across multiple devices, the data is normalized and stored in a relational database. This approach is optimized for detecting alerts, but is less effective when ad hoc queries are necessary to investigate attacks that

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

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

use multidimensional tactics that touch and move from system to system, and may include a multitude of vectors, exploits, and tactics, techniques, and procedures (TTPs).

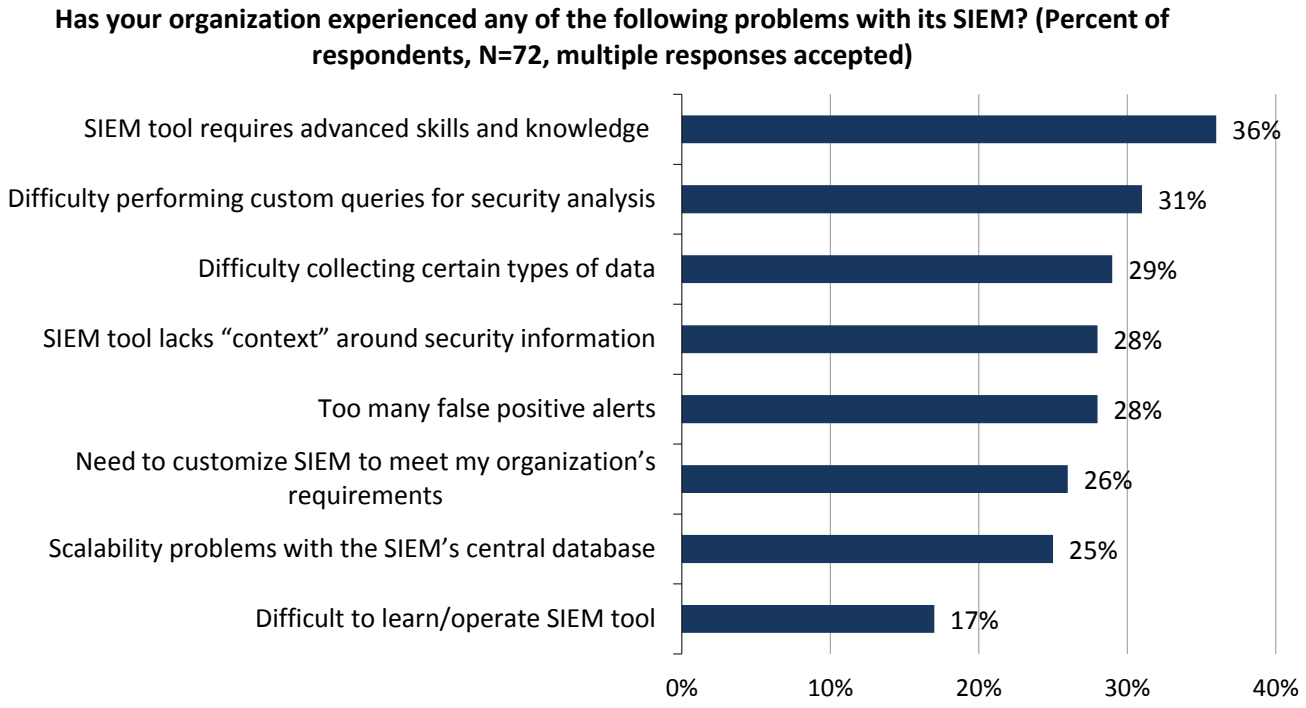
- **SIEM platforms rely on fixed storage (schema).** Most SIEMs operate using a relational database and therefore require that all of the data ingested be predefined prior to loading. The requirement to predefine the data and control how the data is sent to the SIEM via an agent restricts the amount and types of data that can be collected and analyzed. This also requires significant management time for end-users as they keep up with agent updates and change revisions. All of this results in unwanted limitations on the types of security data that analysts see and what they can do with this data once they see it.

- **SIEMs rely on predefined context.** SIEMs' reliance on relational databases demands that any additive context be predefined before solution deployment. As a result, SIEMs struggle with adding additional context such as location, physical security information, role, and identity without significant and expensive customizations. These details could mean the difference between rapid incident detection and a successful low-and-slow attack.

- **SIEMs are inflexible.** Regardless of the industry, no two organizations are the same. All run different technologies, and have unique environmental contexts, security postures, and programs. Out-of-box capabilities and reports are attractive, but most organizations need to customize a SIEM to fit their environment. This entails adjusting existing correlation rules, adding dashboards and reports, or creating new ones. Additionally, nontraditional and customer data sources are often required to combat advanced threats and must be brought into the systems at great expense. In the case of SIEM, time and resources are the enemy of efficient and effective cybersecurity.

In reality, many organizations mostly use SIEM for regulatory compliance and monitoring, rather than security analysis and investigation. This makes it difficult to leverage these legacy systems to address the requirements for defending and responding to targeted multidimensional attacks.

FIGURE 2. SIEM Problems at Enterprise Organizations



Source: Enterprise Strategy Group, 2015.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Enterprises Need a New Approach to Cybersecurity

In the past, information security was really based on event correlation designed for monitoring and detecting known attack patterns. This model alone is no longer adequate as multidimensional cyber-attacks are dynamic and can use different tactics and techniques to find their way into and out of an organization. In addition, the traditional set of security devices is designed and optimized to look for particular aspects of attacks: a network perspective, an attack perspective, a malware perspective, a host perspective, a web traffic perspective, etc. These different technologies see isolated aspects of an attack and lack the bigger picture. This makes cyber-attacks extremely difficult to distinguish or investigate, because until all the event data is combined, it's extremely hard to determine what an attacker is trying to accomplish.

So what's needed? While waging war across Europe, French military and political leader Napoleon Bonaparte stated, "War is 90% information." This prescient observation is certainly true with regard to cyberwar and cybersecurity as well. Addressing new types of cyber-threats requires a commitment to data collection and processing as well as much greater diligence on security data analytics. ESG refers to this as analytics-driven cybersecurity, which includes:

- Casting a wider net on relevant data. Since multidimensional cyber-attacks most likely traverse a multitude of systems, networks, protocols, files, and behaviors, the security team must analyze data across all areas. This means collecting from a wide variety of data sources including logs, flows, network packets, endpoint forensics, identity systems, physical security, etc., and making them available to all members of the security group. Since multidimensional attacks can happen over long time periods, historical analysis must also be incorporated so analysts can perform root cause analysis and attack scoping to determine the breadth of a compromise or data breach.

- Flexible data enhancement. While original data formats should be preserved, security analysts must also have the ability to tag, index, enrich, and query any data element or group of data elements together to get a broader perspective for threat detection/response. Why? This allows the analysts to add context to the raw data, making it more informative and actionable. Furthermore, enhancing the data can help eliminate steps in cyber-investigations and enable junior analysts to triage investigations and become more productive.

- A wide-angle data lens. Like multidimensional cyber-attacks, security investigations tend to be asymmetrical and random in nature. As seasoned security analysts spot anomalies like suspicious traffic egresses in their network, they dig into associated clues such as internal source IP addresses, internal and external connection histories, system changes, etc. The SOC team needs the ability to pivot from one data element to all others using any data field/value in order to follow the chain of evidence from field value to context, tracing the steps the attack has taken. This capability is needed across systems, protocols, network traffic, historical timeframes, etc.

- A quantum improvement in usability. Operations guru W. Edward Deming once stated, "If you do not know how to ask the right questions, you discover nothing." This adage is certainly applicable to cybersecurity as well: Security data will remain a black hole if it can't be easily queried and understood by *all* security professionals—from entry-level staff to highly experienced security analysts. To accomplish this, systems must provide a simple interface and search-based access to broaden and simplify access to data. This will empower junior security analysts to investigate threats and gain valuable experience. Systems should also allow for straightforward ways to create dashboards and reports to streamline security operations. Finally, new systems should offer visual analytics that help the SOC team understand relationships, track historical trends, and pivot across data elements.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

CISOs face a stark reality: The processes and technologies they employed for the last 15 years are no longer enough. Rather than overreact by implementing the cybersecurity silver bullet du jour, savvy CISOs will take a step back and examine the threat landscape. This exercise will reveal the complex nature of modern multidimensional cyber-attacks and likely convince them to adopt a more proactive and comprehensive strategy.

So what's needed? A vast improvement in cybersecurity analytics and intelligence from inside and outside the organization. This means collecting, processing, and analyzing all data and focusing on the people, process, and technology needed to address the post-infection activities. It also includes responding in a coordinated fashion to an incident to investigate and determine root cause; scoping, containing, and remediating the problem; and bringing the learnings of the investigation back into the system for proactive diagnostics and mitigation. In truth, this new approach to cybersecurity can be viewed as an end-to-end relationship between big data security analytics technologies, cybersecurity strategy, and the infosec team's skill set. The technology must become more scalable, and become far easier to use. At the same time, security professionals must learn how to be better incident responders by asking the right questions and knowing how to pivot through investigations.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an integrated IT research, analysis, and strategy firm that is world renowned for providing actionable insight and intelligence to the global IT community.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.