SIEM's Total Cost of Ownership – Key Considerations

Stratecast | FROST & SULLIVAN

Michael P. Suby
Stratecast VP of Research

August 2016

INTRODUCTION

For security analysts, a flow of security alerts is an inevitable consequence of the digital age. Moreover, as alerts can signal business-impacting incidents, the enterprise's security staff cannot be complacent. Staff must be relentless in gathering logs, setting alert parameters, assessing alert severity, and then prudently responding to incidents with countermeasures. This, however, is a demanding responsibility. The broadening range, complexity, and dynamism of the enterprise's network and systems, combined with a well-armed and motivated hacker community, guarantees that security alerts will increase in volume and diversity. Thus, what may have once been a manageable trickle of routine alerts has escalated into a continuous bombardment that few businesses are equipped to reliably tame. Consequently, the mission of security organizations to protect the interests of the business through timely and effective management of security alerts and incident response has tumbled into a state of jeopardy.

Clawing out of this state of jeopardy is possible, but it carries a significant price tag. Upping security staff may seem like a reasonable path, but it automatically adds to the organization's recurring costs (i.e., more personnel on the payroll). Moreover, staffing is linear (i.e., more alerts require more personnel), and recruiting and retaining staff in the long-standing seller's market for security analysts is challenging.

Elevating the security staff's productivity through workflow improvements, so they can dig through the mountain of alerts faster and produce better results (i.e., detecting and responding to severe security incidents with consistent proficiency), is another option, separately or in combination with increased staffing. Workflow improvements, however, are not a panacea, either. First, continuity must be preserved. Current workflows cannot be retired and new workflows adopted without first going through a transitional period where the old and new workflows run in parallel to avoid unintended process gaps. And, the transition period may last longer than planned, and may not produce all of the expected improvements. Most importantly, workflow improvements are dependent on technology tools that directly support people-dependent workflow processes. Notable for security analysts are the tools that automate the prioritization of alerts (e.g., low, medium, and high risk), speed investigations, and shorten the time from assessment to enacting countermeasures. However, if the tools are deficient, there is a cap on the gains sought through workflow improvements and staff additions.

> As the central nervous system in orchestrating security alert assessments and incident response, Security Information and Event Management (SIEM) is a principal determinant in the total cost of these critical security functions.

As the central nervous system in orchestrating security alert assessments and incident response, Security Information and Event Management (SIEM) is a principal determinant in the total cost of these critical security functions.

Furthermore, SIEM platforms directly affect staff productivity and proficiency. In practice, SIEM is either an enabler in reaching a higher tier of productivity and proficiency; or a retardant due to limitations in

adaptability, scalability, automation, user intuitiveness, and analytics—and, as a consequence, a contributor to escalating operational costs.

We believe that organizations that take a holistic view on SIEM platform capabilities and the SIEM's impact on people and process are best positioned to choose a SIEM platform that delivers both resiliency on the business-protection mission and certainty in total cost. To that end, we describe in this paper factors to include in assessing SIEM's total cost of ownership.

SPEED TO VALUE

SIEM's core value is concentrated on speed. Specifically, how fast, with consistent precision, can security analysts uncover and thoroughly investigate security alerts; and how fast can appropriate countermeasures be taken on security incidents, to mitigate business impact.

> Many organizations are losing the race against the hacker community by a large margin.

Unfortunately, many organizations are losing the race against the hacker community by a large margin. As noted in the *Verizon 2016 Data Breach Investigation Report*, the percent of compromises that transpired in "days or less" forms a trend line starting at 72% in 2004, and rises to over 95% in 2015. Over this same time period, the percent of compromise discoveries that occurred in "days or less" also improved from 13% to 23%; a rise, however, that has not narrowed the time gap between compromise and discovery. In other words, the bad guys are accelerating their exploits faster than the good guys are accelerating their ability to discover them.

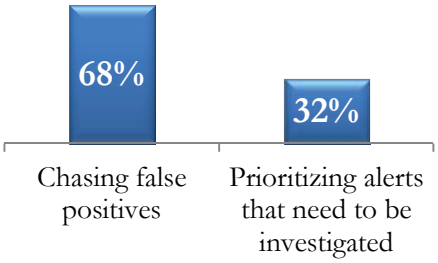
Of the bad guys' tools, phishing has been a particularly rapid means (minutes, not days) to compromise, as is also highlighted in the same breach investigation report:

"The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds. The median time to the first click on the attachment was 3 minutes, 45 seconds."

The window between the point of initial intrusion until the attacker has successfully compromised targeted systems is the time that security analysts must conduct an essential set of preliminary activities. Those activities include:

1. Collecting data (gathering the raw materials)
2. Discarding false positives (peeling away the chaff)
3. Prioritizing alerts (of the remainder, determining what to investigate further)

Best Use of Time?



However, according to the Ponemon Institute in the *State of Malware Detection and Prevention* (February 2016), most organizations are struggling in being efficient in these activities. In particular, 68% of the surveyed IT security

practitioners agree or strongly agree with the statement that they spend a significant amount of time "chasing false positives"; and 32% indicated that they spend a significant amount of time "prioritizing alerts that need to be investigated." In mirrored fashion, the more time spent on these preliminary activities by security practitioners, the more time hackers operate unimpeded.

These circumstances are not unalterable. As discussed in the following two sections, the path to narrowing the time gap between compromise and discovery, and then neutralizing business-impacting incidents, is through a comprehensive and mission-oriented SIEM. Furthermore, a well-designed SIEM will not only advance security objectives, but will also optimize security analysts' time and talent, and streamline workflow processes across partner organizations, including network administration. In turn, SIEM's total cost of ownership is not so much attributable to "ownership" (the hardware and software licensing of the SIEM platform) as in "operations"—that is, directing personnel and process for maximum impact.

Confidently Breezing Through the Preliminary Activities

Rapidly zeroing in on business-impacting incidents is essential, as any time delay is a benefit to hackers. However, this does not need to be an expensive drain on the organization; a well-rounded SIEM should bear the load. In order for this to be the case, the SIEM should, in our opinion, be standardly equipped to accomplish the following:

"Rapidly zeroing in on business-impacting incidents is essential, as any time delay is a benefit to hackers. However, this does not need to be an expensive drain on the organization; a well-rounded SIEM should bear the load."

- **Collect data at scale** – As the lifeblood of security analysis, a wide net of data sources is indispensable in: (1) ensuring that there are no blind spots, and (2) triangulating data from multiple sources to sharpen the precision in alert investigations and response. Furthermore, SIEM must be able to incorporate new data, including both internal system sources and external threat intelligence sources. This must be an out-of-the-box feature, with routinely expanding device support to incorporate the available and valuable data sources of the future. Moreover, this out-of-the-box feature is critical in avoiding cost escalation due to reliance on third-party tools and the additional overhead in reaching a centrally managed data lake. In essence, a SIEM reflects the functionality of a Big Data system.
- **Ingest multiple data types seamlessly** – While a standard format for all incoming data types is desirable, it is impractical to expect it, especially as new data types emerge (e.g., consider the advent of Internet of Things). Therefore, an effective load-bearing SIEM features an extensive inventory of certified data integrations, and built-in parsing rules to place every piece of incoming data into a ready-to-use state (e.g., security technologies, network infrastructure, and data center or cloud environments, servers and applications). If the SIEM is not equipped with a broad collection of log normalization rules, the organization

faces a major "no win" dilemma: incur the expense of writing and maintaining custom processing scripts, disregard data types that could be useful for security monitoring, or undermine analyst productivity by requiring them to bounce among multiple data silos during incident response.

- **Be prepared for the unexpected** – As the number and variety of data sources and types expand, these data waves can potentially tax the SIEM beyond its capacity. Worst case, the SIEM is disabled much like a denial of service attack rendering a website unavailable to legitimate users. Again, in the context of the widening time gap between compromise and discovery, an advantage is ceded to hackers and other adversaries who prey on lumbering, misdirected, or even temporarily offline security operations. Plus, the effort to resurrect a disabled or crashed SIEM and return it to its previous known good state can be time and resource intensive. Recognizing these operational risks and expenses, the SIEM needs to be designed to reliably adjust to data volume swings (e.g., handle data surges without log losses), and be highly available (e.g., no SIEM downtime when additional capacity is being brought online or during a system update).
- **Fluidly expand functionality** – Security operation centers (SOCs) are directly serviced by the SIEM, if not designed around it. And, the functions that SOC personnel performed a few years ago are different from what they must do today (and likely greater in number), and the same will be true in the years ahead. Therefore, a SIEM must be constructed as an open and fluid platform that embraces change, so that new functionality, such as behavioral anomaly detection, can be modularly added by the SIEM vendor. This needs to happen without major retooling, and without forcing current security analysts to become proficient with new functionality, or requiring recalibration to a new system interface. The proof of this expandability is not only in an expandable architecture, but confirmed by vendor actions. If the SIEM vendor has not demonstrated a history of "innovation as a practice," there is little likelihood that the future will be different.
- **Systematically reduce the number of alerts** – Generating more alerts, driven by more data and functionality, is not necessarily desirable. In fact, more can be overwhelming and counterproductive. A load-bearing SIEM is equipped with effective alert filters and automated cross-correlation algorithms. These reduce security personnel's ground work of conducting cursory analysis on thousands of alerts, too often to discard false positives, in order to arrive at a more manageable number. Correspondingly, these same features assist in granular risk-based monitoring. Operationally, not only do these features lower resource and time requirements by substituting technology for human involvement, but they also ultimately direct more security analyst talent to the core objective of mitigating incidents before real damage occurs. If the SIEM vendor does not have a history of dedicated attention to alert filtering and cross-correlation, the SIEM is not mission-oriented.

Competing for the Gold Medal

With the preliminaries of SIEM confidently addressed, our focus now turns to the SIEM attributes that further enhance the organization's proficiency and productivity in supporting its security mission, while remaining cost-efficient. Again, it is the design of the SIEM that makes the difference. Following are the design attributes we consider most relevant, which we have organized into three themes: security analyst productivity, collaborative workflows, and servicing multiple objectives.

Security Analyst Productivity

With automatically vetted alerts, the security analyst can now get down to the business of investigating and determining severity, urgency, cause, and countermeasures. This is still no easy task, but it is definitely less burdensome now that the previous mountain of alerts has been systematically winnowed down. This enables thoughtful investigations on fewer alerts, resulting in conclusions with higher confidence and pinpoint countermeasures. Directly supporting these outcomes are our recommended SIEM attributes that contribute to the productivity of security analysts:

- **Unified system interface** – Swivel-chair movement between multiple system interfaces, to collect and correlate disparate data, is a productivity robber. This type of forced analyst effort consumes precious time, introduces potential error, and impacts post-incident forensic investigations. A better approach is a unified system interface—a single intelligent cockpit.
- **Intuitive analyst workflow** – Even with a unified system interface, the work of the security analyst, and the SIEM itself, can still be highly complex. Left unchecked, this complexity contributes to a learning curve for security analysts that is longer, and organizational reliance on unique skill sets that is greater, than each should be. Given the tight labor market in the security discipline, organizations need to move security analysts up the learning curve quickly; and effectively cover their operational exposure when staff departures occur. Intuitive analyst workflows supported by the SIEM serve to meet these objectives.
- **Instant script development** – Analyst observations of "seen this before" and "as seen by a colleague" are rich opportunities to improve analyst productivity by automating repetitive tasks through scripts; such as initiating a full forensic scan of an endpoint, or disabling a compromised credential. Furthermore, by-default recording of the analyst's task sequences, and comparison to existing scripts, paves the way to quickly building a robust catalog of scripts that can be leveraged across the entire team of security analysts. For new team members, this script catalog also increases their coming-up-to-speed trajectory.
- **Fast and precise search** – The SIEM must empower personnel to find very specific data. Enabling users to perform both unstructured and targeted contextualized searches empowers personnel to approach questions from diverse angles, and eliminates the need for advanced scripting skills. The significant factor then becomes how quickly data is returned to the analyst, because time spent waiting is time wasted.

Collaborative Workflows

In the previous section, we focused on SIEM attributes that strengthen the productivity and proficiency of individual security analysts. While critical, analysts do not and cannot work in isolation. Risk management is a communal effort, and collaborative workflows supported by the SIEM create beneficial synergies among the entities that have vested interests. We placed these SIEM -supported collaborative workflows into three categories: among analysts; with supervisors; and with other vested entities.

> Risk management is a communal effort, and collaborative workflows supported by the SIEM create beneficial synergies among the entities that have vested interests.

- **Among analysts** – Hackers operate as a community. They buy, sell, and trade tips about their craft. Security analysts responsible for uncovering and mitigating the actions of hackers must also learn from the talents of each other in order to combat the community strength of hackers. For that, the SIEM should be the center of seamless collaboration among the analysts. SIEM-centered collaboration includes: real-time visibility into the actions of other analysts, the means to allow group collaboration on a single incident, and the means for analysts to easily insert files and screenshots into their cases. Moreover, there should be no reason for analysts to jump out of the SIEM to use off-the-shelf collaborative tools (another form of productivity-robbing swivel-chair movement). And, as natively part of the SIEM, complete documentation of analyst actions, and supporting materials, are preserved for post-incident forensics and in support of professional education.
- **With supervisors** – Supervisors of security teams need their analysts to consistently operate at a high level of proficiency and productivity, both individually and collectively. The previously outlined SIEM attributes are aligned with this objective. The supervisor also has the responsibilities of: (1) ensuring that attention on high-priority alerts does not waver due to shift and personnel changes, and (2) assigning alerts, cases, and incidents to analysts. These are not insignificant tasks, in light of the unpredictability in alert volume and complexity, even after the alerts have been systematically vetted. Automatic recording and electronic documentation built into the SIEM support gapless knowledge transfers across shifts and personnel, and reduce supervisory effort. Also, alert status, duration spent at each stage of alert processing, and other operational measurements presented in a dashboard with drill-down capabilities, provide supervisors with the at-a-glance views needed to confirm progress and recognize issues on a timely basis. This is certainly a saner and more effective means of operating than gathering and assembling this information manually, or straddling multiple data silos. Another feature, automatic assignment of alerts based on supervisor-defined criteria (e.g., analyst tenure and skill profile), reduces the potential of unassigned (and therefore unaddressed) alerts; and ensures that each analyst receives an equitable share of the workload, even when the supervisor is unavailable. Collectively, SIEM as an automated workflow coordinator, as described, mitigates breaks in operational continuity and streamlines supervisory duties.
- **With other vested entities** – Determining the countermeasures of an incident response is only half the battle—the countermeasures must then be enacted. Not uncommonly, however, the decision to enact a countermeasure is not solely within the security analyst team's authority; approvals from other organizations are needed as a safeguard to avoid unintended consequences to other business functions. Seeking approvals through a manual or a bespoke process interrupts what was otherwise a fully in-system approach; introduces potential errors and misinterpretations; and adds time—time the adversaries will leverage. A flexible and automated countermeasure approval process should be self-contained in the SIEM. Full documentation supporting the countermeasure is present for all approvers to view; approvers can interact with the analyst through the same in-system collaboration tools previously noted; and a complete electronic audit trail is automatically created. Additionally, a SIEM with this capability will start out with a library of standard countermeasures that the organization can either use as is or modify for their particular circumstances. Certainty about the expected outcomes of standard countermeasures (and avoidance of unexpected outcomes) provides the confidence necessary to streamline and speed the approval process.

Servicing Multiple Objectives

Gaining more mileage from each dollar spent is an enduring mantra of business. This same mantra applies to SIEM. Considering all the capabilities and features we have outlined in SIEM's systematic support of alert management and incident response, SIEMs of this caliber are equipped to service additional objectives. They include:

- **Automate compliance adherence** – Demonstrating regulatory compliance and supporting audits have long been a natural fit for SIEMs. The meaningful difference with the type of SIEM we described is in lowering the effort required. The comprehensiveness of time-stamped electronic records implicit in this type of SIEM—logs, investigative activity and conclusions, and countermeasures—automates the compiling and reporting process with a seal of integrity. And with automation, demonstrating compliance can then pivot from being a periodic event to a continuous process, without elevating personnel involvement or taking personnel away from their routine activities. Even if real-time compliance assurance is not required, additional monitoring can identify and resolve compliance issues before they become serious offenses.
- **Monitor IT operations** – Also historically aligned with SIEM, but not as tightly as compliance, the ability to monitor IT operations becomes more tangible as the SIEM's data collection and analysis capabilities expand. A single data repository and analytics engine provides the potential for organizations to stretch their IT and security budgets.
- **Gather intelligence on attackers** – Successful targeted attacks show that commercial threat intelligence services may be insufficient to provide the cyber awareness that organizations need to protect themselves. A SIEM's holistic view of an organization's environment can enable the generation of internal intelligence, which can be correlated with or compared to external threat intelligence services. Additionally, in an increasingly partner- and supplier-connected business environment, this specialized intelligence can assist in detecting targeted attacks originating from "trusted" entities.

THE LAST WORD

SIEM's total cost of ownership is heavily weighted on operations—the people and processes that rely on and are enabled by the SIEM platform. As such, the total cost of SIEM, to no small degree, is dependent on the platform's enduring attributes; that is, attributes that have a lasting impact on an organization's cost efficiency in effectively managing risk.

In our view, the SIEM attributes that exert the greatest influence on cost efficiency and cost predictability are:

- Comprehensiveness in functionality, from data collection through sophisticated analytics and countermeasures
- Obsessive attention to workflow automation and resource productivity
- Modularity, so adapting to whatever the future brings is not just possible, but planned
- Out-of-the-box embedded expertise; the SIEM is an expert-enabling security analytics system

In evaluation of SIEM platforms, either in a first deployment or as a replacement to an existing SIEM, these attributes should be front and center on the scorecard.

Michael Suby

VP of Research
Stratecast | Frost & Sullivan
msuby@stratecast.com

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT STRATECAST

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion