sumologic

A Sumo Logic White Paper

Has SIEM Lost Its Magic?

Top five reasons why SIEMs are failing security professionals

Security information and event management (SIEM) solutions have been around since 2000, and they were developed with the goal of helping organizations in the early detection of targeted attacks and data breaches. Needs cut across analyzing event data in real time to the collection, storage and analysis of log data for incident forensics and regulatory compliance. While these solutions hold out tremendous promise, are they failing to deliver? Has SIEM lost its magic?

> According to a recent Gartner report written by Oliver Rochford implementing SIEMs continues to be fraught with difficulties, with failed and stalled deployments common.[1]

According to a recent Gartner report written by Oliver Rochford implementing SIEMs continues to be fraught with difficulties, with failed and stalled deployments common.[1]

In fact, our two co-founders – Christian Beedgen and Kumar Saurabh – came from ArcSight, where they served in the capacity of Chief Architect and Director of Engineering, respectively. They were looking to build something that would address many of these shortcomings and deliver real value to customers.

Main Pain Points

+ **Time to value** – Protracted time to value, which is common with large-scale on-prem deployments, in no longer acceptable to many enterprises, which are being asked to drive the business forward, faster, and oftentimes with less resources and budget. In the book Consumption Economics, organizations that do not help customers get the most value from their technology investment, within a reasonable time period, will be disrupted. "Left behind will be a trail of former big-name tech brands still trying to hand off hard-to-implement, hard-to-consume solutions to their customers' understaffed IT departments, hoping for the best."[2]

  As an example, a recent SIEM research report by the Ponemon Institute,[3] found the average length of time to fully implement a SIEM across the enterprise was 15.2 months.

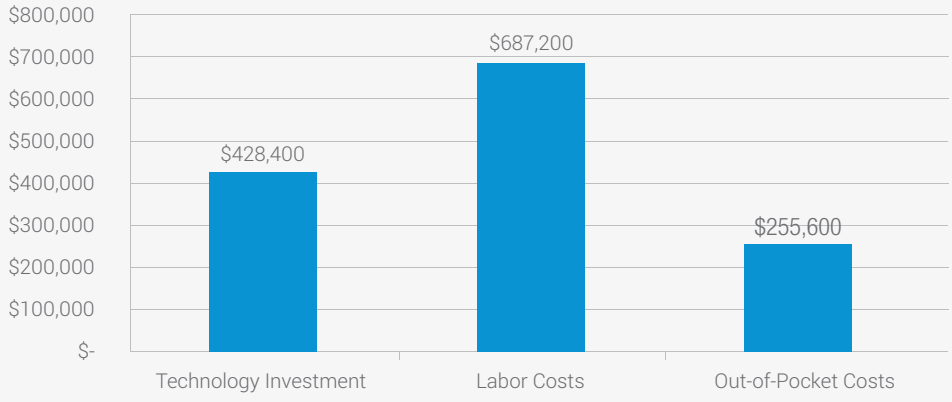
  We are already starting to see this shift among many of our new customers who came to us from legacy SIEM solutions looking for technologies that delivered more value, more speed, less pain.

- **Scalability** – Trying to scale and support growing, and often unpredictable log volumes becomes very problematic for on-prem solutions. The term "auto-scaling" is just not part of the SIEM on-prem vernacular. What would happen to a retailer during a Black Friday? Or an airline reservation system during the holiday travel season? To address this, these systems need to be architected to handle max loads volumes, which take time to plan, architect and build, as well as adding a tremendous amounts of cost, only to see capacity sit idle when volumes drop off. CAPEX expenditures like this are a hard pill for modern day CISOs to swallow.
- **Lack of Visibility** – At a recent AWS Enterprise Summit in NYC, I had the opportunity to hear the CISO of Medidata Solutions discuss his search for a SIEM solution and was considering two Gartner 'Magic Quadrant Leaders'[4]. Medidata Solutions is a Life Sciences organization that runs clinical trials for pharmaceutical and medical device companies. Their solutions operate in the AWS cloud. When discussing with these on-prem "Magic Quadrant leaders" how they could support visibility, security and compliance for mission-critical workloads running on AWS, he realized it was going to be a very short conversation and vetting process.

  Additionally, with on-prem solutions, organizations do not have visibility into what their customers are regularly doing to address known and emerging security incidents and how customers continue to use their solution on an ongoing basis to drive value. How can any company grow and evolve their product or service offering to better address customer needs without these insights?
- **Management Overhead** – Managing the execution environment requires a lot of work and resources. Hardware and software needs to be procured and configured, network devices need to be architected and deployed at critical infrastructure points, user access controls need to be established, databases need to be set up and optimized for the expected performance and load, and the list goes on. Not only are we seeing companies struggling to hire top notch security professionals - who often seem to be in short supply - security, operations and development teams would much rather focus on driving the business forward, increasing competitive advantage, building stronger experiences for their customers - NOT having half their available time consumed by managing the execution environment.
- **Cost** – In the same SIEM research report by the Ponemon institute[3], the extrapolated average cost incurred by interviewees' companies to deploy QRadar across the enterprise is as follows:

Bar Chart 3: Extrapolated average cost spent on SIEM

Analysis conducted from 25 confidential interviews of QRadar users



Adding up Technology Investment, Labor Costs and Out-of-Pocket expenses, organizations need to budget over $1.3M!

The SIEM market sort of reminds me of the Data Loss Prevention (DLP) market over the last decade. Dominated by the likes of Symantec (who acquired Vontu), people would spend millions of dollars for all the various network and endpoint discovery, monitoring and prevention modules and tons of consulting dollars to set up, customize and get the engine going (sound familiar?). But in the end, it failed to live up to its promise - it lost its magic. This failure saw the rise of DLP-light solutions and DLP capabilities that were merged into endpoint and email/web gateway protection suites. This ultimately caused the demise of stand alone, enterprise DLP solutions.

> "The average length of time to fully implement a SIEM across the enterprise was 15.2 months, with the average costs exceeding $1.3M.

I am not sure what the future holds for SIEM, but it is not what currently exists. A reformation of some sort will surely need to happen.

We are already starting to see the emergence of purpose-built cloud-based services that support advanced security analytics and compliance use cases. These solutions leverage machine learning and are not constrained by rigid, fixed rule sets that fail to uncover new and emerging security events. Being able to understand what is normal within the scope of the security infrastructure, and notify security operations personnel when patterns and behaviors deviate from that baseline – automatically – that is when the magic starts to happen.

Sources:

1. Overcoming Common Causes for SIEM Deployment Failures, 21 August 2014, G00260858
2. Consumption Economics, The New Rules of Tech, by J.B. Wood, Todd Hewlin and Thomas Lah
3. IBM QRadar Security Intelligence; Independently conducted by Ponemon Institute LLC, February 2014
4. Gartner lists the following five vendors as leaders in the Magic Quadrant for SIEM, published July 20, 2015: IBM, HP, Splunk, Intel Security and LogRhthym

About the Author

Mark Bloom is a Data Security veteran with over 10 years experience in a variety of industries. Mark has achieved noteworthy success in his time with Trend Micro, IronPort (acquired by Cisco), SonicWALL (acquired by Dell), MailFrontier (acquired by SonicWALL) and Compuware. He is now the Director of Product Marketing, Compliance and Security at Sumo Logic.

305 Main Street
Redwood City, CA 94063
www.sumologic.com