RKON

SOLUTION PAPER

Finally, The Time for Security Information Event Management (SIEM)

Marc Malizia
Co-founder & CTO
RKON Technologies

"…there are now SIEM products capable of being installed and delivering useful data within a few weeks."

Security Information Event Management (SIEM) tools have been around for a long time. My first encounter with a SIEM vendor was about twenty years ago while being courted to resell their product. To this day, I still recall two vivid memories from that meeting: the product was very complex and quite costly to buy and implement.

I will never forget the salesman boastfully telling me the product would be great to help drive our service business. He went on to brag about the fact that for every dollar of software sold, four dollars of service revenue would be required to implement. Promptly I inquired as to the average deal size. Again, he proudly answered the software portion was $500,000 to which $2 million in services cost would be required. Well, as nice as that sounded, red flags began flaring in my head like fireworks, leading to the thought that software requiring that level of service to implement was probably way too complex for the typical enterprise to implement and definitely not manageable on a day-to-day basis and thus would most likely end up as shelf ware. I never did partner with that vendor and in fact stayed clear of all SIEM solutions during that time. My initial assessment was validated as our customers relayed stories of their failed or stalled SIEM projects.

The Time Has Come

Fast forward twenty years and a light at the end of the SIEM tunnel seems to have appeared. The time has come for SIEM implementations to live up to their initial promises and deliver increased security and a return on investment. The optimism is based on the following three reasons: maturity of products, availability of cost-effective solutions and increasing compliance concerns.

After a twenty-year incubation period there are now SIEM products capable of being installed and delivering useful data within a few weeks. This is mainly due to the fact that these products now have an abundance of predefined correlation rules which dramatically ease the setup while reducing the customization required. Though greatly improved, there are still products out there that market themselves as "easy" while requiring a team of coders to create correlation rules – buyer beware. If possible, engage a trusted security partner to help navigate these waters and guide you to the appropriate SIEM. Even with a great SIEM product, an experienced partner will take a few weeks to implement and customize a SIEM to the point where useful data is not cluttered by a plethora of false positive entries. Even at this point, continued fine tuning will be needed over the next 60-90 days to attain an optimal state.

SIEM SaaS Solutions

Some services greatly reducing the cost and staffing requirements of SIEM are SIEM SaaS (Software as a Service) and Managed SIEM solutions. By leveraging a SIEM SaaS solution, companies can reduce the burden of implementing and maintaining the base SIEM software platform. Typically, with SIEM SaaS, the customer merely installs a SIEM agent on their servers or directs the log files to the SaaS provider. Though the customer is still required to perform the task of policy setup and optimization, which should not be underestimated, at least some of the work is offloaded to the SaaS provider making for a more palatable undertaking. In the case of a fully managed SIEM solution, the managed service provider assumes the responsibility of getting the SIEM implemented, optimized and in most cases performs the initial incident response and forensic analysis. This path, though more expensive than SIEM SaaS solutions, provides the customers with many advantages. Besides the implementation and tuning now being one hundred percent handled by the provider, the monitoring and incident response role is also assumed by the provider. This greatly reduces the security staffing requirements and thereby cost while providing the hard to find security skills required on a 24/7 basis. For a mid-sized company, the staffing cost alone on a SIEM implementation can be a deal breaker.

Compliance Requirements

In today's market, the most common reasons for SIEM is to address compliance requirements. Though many of the regulations like HIPAA and PCI have been around for awhile it appears that the auditors are now digging deeper into the technology infrastructure side of the IT shop and demanding proof of the required controls. By providing the ability to maintain logs, alert on breaches, enable incident response and forensic analysis, SIEM has become an integral piece of any compliance plan.

Though my perception of SIEM has changed and I believe it can deliver on the value promised years ago, I do not want to leave you with the perception that SIEM is now a simple solution that provides business value out of the box. Along with the heightened interest in SIEM are vendors trying to jump on the bandwagon and retro-fit their security product to be a SIEM. Most of these products do require sophistication and months of work to get implemented and optimized as they have not undergone the maturation process of the other products. Also, leveraging a partner with experience implementing SIEM can greatly reduce the speed of execution for these projects and deliver a solution which provides a high degree of value. In many cases, outsourcing the SIEM solution to a managed service provider can enable a company to improve their security and meet compliance in a cost effective and efficient manner.

Article was featured in PowerSource (May 2016) and on CloudTweaks.com (March 2016)

Marc Malizia is co-founder and CTO of RKON Technologies, responsible for the company's overall technical vision and strategy. Since helping start the company in 1998, Malizia has played a key role in creating many of RKON Technologies' products and professional service offerings, as well as building the company's internal computing platform, which serves as the basis of the brand's cloud and managed services portfolio. Malizia holds a bachelor's degree in computer science and mathematics from University of Illinois and a master's degree in telecommunications from DePaul University