"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 2
The journal is indexed in: PROQUEST / DOAJ / Crossref / EBSCOhost / INDEX COPERNICUS / DRJI / OAJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Academic Keys/ ROAD Open Access / Academic Resources / Scientific Indexing Services / SCIPIO / JIFACTOR

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT SOLUTIONS) IMPLEMENTATIONS IN PRIVATE OR PUBLIC CLOUDS

Vlad-Mihai COTENESCU[1]

[1] Eng. Military Technical Academy, Bucharest, Romania

Abstract: *The underlying principle of a **SIEM** system is that relevant data about an enterprise's security is produced in multiple locations and being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary.*
*Today's security threats are dynamic in nature and exploits are constantly evolving. Attackers grow more organized, precise and persistent and have access to various automated tools that can trigger very sophisticated attacks. As **threats**and security events evolve, SIEM vendors and the information securitycommunity must work together to build relevant and actionable businessanalytics into their systems. By continuously improving recommendationsand the controls to support those recommendations, SIEM products canbecome true information security hubs that not only automate audits butalso provide proactive means to protect the organization. SIEMtechnologies for **centralization** and consolidation of an organization'ssecurity data will continue to be important investments for organizationswanting to accurately **respond** to threats and ultimately improve their riskand compliance postures.*
*In the field of computer security, security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of **security alerts** generated by network hardware and applications.*

Introduction:

Security Information and Event Management Solutions have been around since the year 2000 and have continuously to keep up with the rapid change in public and private technology-based environments. With the increase in processing resources and the evolution in network speed and storage capabilities the need to support devices evolved in different form factors, many of which IT doesn't directly control. Organizations add new applications on a monthly basis in public or private cloud environments and leverage virtualization technologies and SaaS for increased efficiency. In current days IT and information security professionals are expected to provide, with much less control, access anywhere while maintaining accountability, confidentiality and integrity of the data.

If that wasn't enough, bad things are happening much faster. Not only are our businesses always on, the attackers don'ttake breaks, ever. New exploits are discovered, 'weaponized', and distributed to the world within hours. So we need tobe constantly vigilant and we don't have much time to figure out what's under attack and how to protect ourselves beforethe damage is done. Compound these 24/7 demands with the addition of new devices implemented to deal with newthreats. Every device, service, and application stream zillions of log files, events, and alerts.

The real issue is pretty straightforward: of all the things flashing at us every minute, we don't know what is reallyimportant. We have too many data, but not enough information.

This plentitude of data needs to be normalized and correlated in order to become meaningful and actionable.

Security Information and Event Management (SIEM) and Log Management tools have emerged to address these needsand continue to generate a tremendous amount of interest in the market, given the compelling use cases for thetechnologies.

Hypothesis:

Historically, SIEM consisted of twodistinct offerings: SEM (security event management), which collected, aggregated and acted upon security events; andSIM (security information management), which correlated, normalized and reported on the collected security event data.

These days integrated SIEM platforms provide near real-time monitoring of network and security devices, with the idea ofidentifying the root causes of security incidents and collecting useful data for compliance reporting. Most end usersbelieve the technology is at best a hassle and at worst an abject failure. SIEM is widely regarded as too complex, and tooslow to implement, without providing enough customer value to justify the investment.

While SIM & SEM products focused on aggregation and analysis of security information, Log Management platformswere designed within a broader context of the collection and management of any and all log files. Log Managementsolutions don't have the negative perception of SIEM because they do what they say they do: aggregate, parse, andindex logs.

DOI: 10.21279/1454-864X-16-I2-058

Log Management has helped get logs under control, but under-delivered on the opportunity to derive value from thearchives. Once again: more data, less information. Collection, aggregation, and reporting are enough to check thecompliance box, but not enough to impact security operations — which is what organizations are really looking for. Endusers want simple solutions that improve security operations, while also checking the compliance box.

In an organization's environment, depending on its size, you might have devices ranging from the tens to maybe thousands that need to be managed, monitored and constantly updated. These devices can reside in a private cloud or might be sitting in a public cloud that permits the rapid use of resources. To understand how these environments work we would need to define their core attributes: multitenancy (shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources.

Multitenancy (shared resources):

Unlike previous computing models, which assumed dedicated resources (i.e., computingfacilities dedicated to a single user or owner), cloud computing is based on a business modelin which resources are shared (i.e., multiple users use the same resource) at the networklevel, host level, and application level.

Massive scalability

Although organizations might have hundreds or thousands of systems, cloud computingprovides the ability to scale to tens of thousands of systems, as well as the ability tomassively scale bandwidth and storage space.

Elasticity

Users can rapidly increase and decrease their computing resources as needed, as well asrelease resources for other uses when they are no longer required.

Pay as you go

Users pay for only the resources they actually use and for only the time they require them.

Self-provisioning of resources

Users self-provision resources, such as additional systems (processing capability, software,storage) and network resources.

Interest in the cloud is growing because cloud solutions provide users with access tosupercomputer-like power at a fraction of the cost of buying such a solution outright. Moreimportantly, these solutions can be acquired on demand; the network becomes thesupercomputer in the cloud where users can buy what they need when they need it. Cloudcomputing identifies where scalable IT-enabled capabilities are delivered as a service tocustomers using Internet technologies.

Using IaaS or SaaS public clouds introduce a series of security and non-security concerns. One of the biggest concern is that all the visibility in the systems provisioned in the cloud is lost. In order to mitigate this shortcoming,organizations need to have the opportunity to either install or leverage an existing vendor solution that offers features like:

- Log Aggregation — Collection and aggregation of log records from the network, security, servers, databases, identity systems, and applications.
- Correlation — Attack identification by analyzing multiple data sets from multiple devices to identify patterns not obvious when looking at only one data source.
- Alerting — Defining rules and thresholds to display console alerts based on customer-defined prioritization of risk and/or asset value.
- Dashboards — An interface which presents key security indicators to identify problem areas and facilitate investigations.
- Forensics — The ability to investigate incidents by indexing and searching relevant events.
- Reporting — Documentation of control sets and other relevant security operations and compliance activities

There are different types of implementations of cloud computing technologies. These technologies can be categorized depending on the limitations introduced when it comes to the network and application management responsibilities.

In an IaaS model (see figure 1 for an architectural diagram example)the vendor provides the entire infrastructure fora customer to run his applications. Often, this entails housing dedicated hardware that ispurchased or leased for that specific application. The IaaS model also provides the infrastructureto run the applications, but the cloud computing approach makes it possible to offer a pay-perusemodel and to scale the service depending on demand. From the IaaS provider's perspective,it can build an infrastructure that handles the peaks and troughs of its customers' demandsand adds new capacity as the overall demand increases. Similarly, in a hosted application model, the IaaS vendor can cover application hosting only, or can extend to other services (such asapplication support, application development, and enhancements) and can support the mostcomprehensive outsourcing of IT.

DOI: 10.21279/1454-864X-16-I2-058

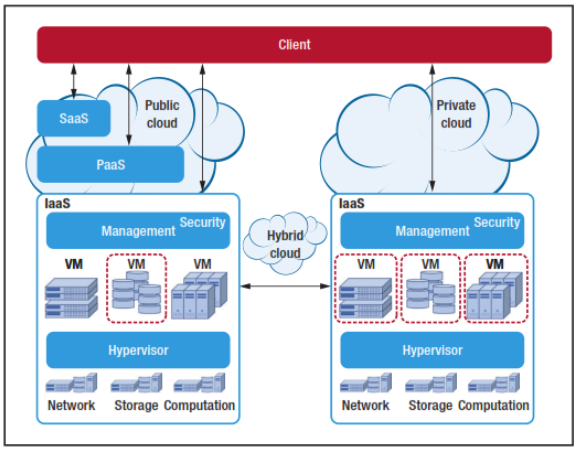

Fig.1 IaaS architecture

In a SaaS model (see figure 2 for an architectural diagram example), the customer does not purchase software, but rather rents it for use on asubscription or pay-per-use model (an operational expense, known as OpEx). In some cases,the service is free for limited use. Typically, the purchased service is complete from a hardware,software, and support perspective. The user accesses the service through any authorized device.

In some cases, preparatory work is required to establish company-specific data for the serviceto be fully used and potentially integrated with other applications that are not part of the SaaSplatform.

Key benefits of a SaaS model include the following:

- SaaS enables the organization to outsource the hosting and management of applications to a third-party (software vendor and service provider) as a means of reducing the cost of application software licensing, servers, and other infrastructure and personnel required tohost the application internally.
- Applications delivery using the SaaS model typically uses the one-to-many delivery approach, with the Web as the infrastructure. An end user can access a SaaS application via a web browser; some SaaS vendors provide their own interface that is designed tosupport features that are unique to their applications.
- SaaS enables software vendors to control and limit use, prohibits copying and distribution, and facilitates the control of all derivative versions of their software. SaaS centralized control often allows the vendor or supplier to establish an ongoing revenue stream with multiple businesses and users without preloading software in each device in anorganization.

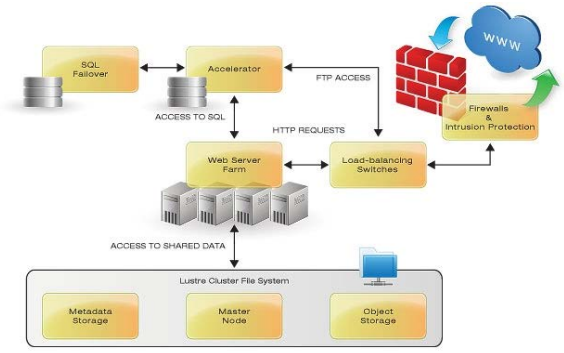

Fig. 2. SaaS Architecture

In all of these cloud implementations, we might have a multitude of applications or systems that got migrated from the private cloud. For all these systems an organization needs to introduce some sort of centralized monitoring that can be achieved by standing up a cloud SIEM aggregator. As seen in figure 3 an integration between a public cloud SIEM solution and a private cloud SIEM solution is essential. The role of the cloud SIEM aggregator is to, as the name says, aggregate and normalize all the security and non-security events generated by the cloud applications and servers. Once these event logs are being stored they need to be kept, depending on the organization need, a period ranging from 3 to 12 months. The role of the aggregator is also to convert the logs into a meaningful format that can be processed by the private cloud solution.

All the logs that are being stored in the public SIEM need to be forwarded via a one-way communication to the private cloud SIEM. Once the data reaches the main, private SIEM solution then it can be correlated with the events generated by the on-premise/private cloud infrastructure.

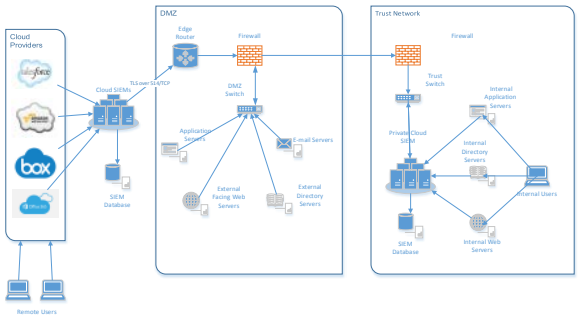

Fig. 3 Public/Private Cloud SIEM Architecture

By having this integration of the environment the organization will have a lot of benefits that include:

- Easier ways to make sure you are compliant with industry rules and regulations
- Increased visibility into the public cloud infrastructure

DOI: 10.21279/1454-864X-16-I2-058

- Better integration between the public and private cloud
- Better Operational Support
- Zero-day Threat Detection
- More control over monitoring and correlation of events across an organization
- Provision of forensic and analytical tools to gain a betterunderstanding of attacks

Other Benefits of SIEM include:

- Increased employee productivity and process efficiencies
- Less manual resources needed for reporting
- Better security situational awareness
- Ability to embrace new trends such as BYOD and mobile working
- Prioritize and protect security investments
- Gain an improved understanding of security threats
- Allow the integration of SIEM with firewall and IPS for rapid incident response
- Centralize and have better control over the enforcement ofIT security policies

BIBLIOGRAPHY

[1] Mather, Tim; Kumaraswamy, Subra; Latif, Shahed, *Cloud Security andPrivacy*, O'reilly, 2009. **ISBN: 987-0-596-802769**
[2] Gartner Research: Hype cycle for cloud computing, 2011
[3] ecfirst, Security Information EventManagement (SIEM) solutions, 2014

DOI: 10.21279/1454-864X-16-I2-058