# Analysis of SIEM Systems and their Usage in Security Operations and Security Intelligence Centers

Natalia Miloslavskaya
*National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)*
*NGMiloslavskaya@mephi.ru*

**Abstract**
To achieve business objectives, to stay competitive and to operate legally modern organizations of all types (e.g. commercial enterprises, government agencies, not-for profit organizations), different size and sphere of activity need to match a lot of internal and external requirements. They are called compliance regulations and mean conforming to a rule, such as a specification, procedure, policy, standard, law, etc. These organizations need to ensure valuable assets, uninterrupted business operation (processes), reliable data and differentiated quality of service (QoS) to various groups of users. They need to protect their clients and employees not only inside but also outside organization itself in connection with which two new terms were introduced – teleworking or telecommuting. According to Gartner by 2020, 30 % of global enterprises will have been directly compromised by an independent group of cybercriminals or cyberactivists. And in 60 % of network breaches, hackers compromise the network within minutes, says Verizon in the 2015 Data Breach Investigations Report. An integrated system to manage organizations' intranet security is required as never before. The data collected and analyzed within this system should be evaluated online from a viewpoint of any information security (IS) incident to find its source, consider its type, weight its consequences, visualize its vector, associate all target systems, prioritize countermeasures and offer mitigation solutions with weighted impact relevance. The brief analysis of a concept and evolution of Security Information and Event Management (SIEM) systems and their usage in Security Operations Centers and Security Intelligence Centers for intranet's IS management are presented.

*Keywords:* SIEM, Security Operations Center, Security Intelligence Center, information security, information security incidents

# 1 Introduction

IS incident refers to a single or a series of unwanted or unexpected IS events that have a significant probability of compromising business operations and threatening (ISO27000, 2016). In turn IS event is an identified (observed) occurrence of a system, service or network state indicating a negative consequence such as a possible breach of IS, policy, standard security practice or failure of controls, or

a previously unknown situation that may be security relevant. IS events may be considered as a part of one IS incident, while the IS incident as a set of IS events. Any attack on a system, service or network can be classified as an IS event or incident. It is vital to know which IS threats exist at the moment, how they could grow into an IS incident and then affect an organization, especially if they could result in exposure of intellectual property and confidential data or service interruption, jeopardize its reputation or financial well-being, etc. So a specialized Security Operations Center (SOC) with the right information protection tools (IPTs) and skilled staff in place as a heart of a good IS incident management has been appeared in the late 1990's. After that a Security Intelligence Center (SIC) with an integrated IS architecture providing full visibility and control and context-driven security intelligence in one place to temporarily deal with network-level and more important higher-level IS events has appeared in 2010. In majority of cases SOCs and SICs are based on Security Information and Event Management (SIEM) systems as their integral part.

Our goal is to compare SIEM 1.0 and SIEM 2.0 and their usage in SOCs and SICs. As a preparatory stage for creating our own Network Security Intelligence Center in the future, we systematize their main features and follow their evolutionary design logic. For that purpose the remainder of the paper is organized as follows. SIEM concept is introduced in Section 2. SEIM 1.0-based SOCs and SIEM 2.0-based SICs are briefly analyzed in Sections 3 and 4 respectively. The future research area concludes the paper.

# 2 SIEM concept

IPTs can register millions of IS events of different origins and consequences in the intranets of large organization during one day only. The amount of work required to identify the truly important data from the viewpoint of IS events and to obtain information on IS incidents can be extremely large. Unfortunately, this activity, often manual and time-consuming, can overwhelm the most experienced professionals.

The automated systems (software) for IS event management – SIEM systems – are used to solve the problem of flow control of the IS events coming from IPTs and to computerize IS incident management process. These systems are crucial for organization's IS. All sizes organizations typically need a SIEM system for compliance purposes to automatically generate reports that provide evidence of the organization's adherence to various compliance requirements. To completely and correctly perform assigned tasks SIEM systems require frequent tuning and customization as they serve in constantly changing, dynamic environment. The indicators (in the form of corresponding patterns) of intranet's resources compromise are deployed as alerts in SIEM systems.

The term SIEM itself has been introduced by the research and consulting company Gartner in 2005. SIEM evolutionary replaced the two types of systems that have historically emerged before them – Security Information Management (SIM) and Security Event Management (SEM) systems (IBM, 2010).

SIM systems provided long-term storage in a centralized repository, trend analysis and automated reporting based on their log lists.

SEM systems collect events in real time, conduct their near real-time analysis, send notifications and represents information at an operator's console to take defensive actions more quickly. Thus, SEM is oriented to immediacy, while SIM is more oriented to historic record keeping.

A combined SIEM system collects logs and other IS-related information for analysis.

The key functions of these three systems can be summed up as follows:

- SIM – log collection, archiving, historical reporting and forensics;
- SEM – real-time reporting, log collection, normalization, correlation and aggregation;
- SIEM – log collection, normalization, correlation, aggregation and reporting.

Log collection of event records from various intranet's sources provides computer forensics tools and helps to address compliance reporting requirements. Normalization maps log messages from numerous systems into a common data model, enabling the organization to connect and analyze related events despite of their initially different log source formats. Correlation links logs and events from disparate systems or applications, speeding detection of and response to IS threats. Aggregation reduces the volume of event data by consolidating duplicate event records. Reporting presents the correlated, aggregated event data in real-time monitoring and long-term summaries.

Typical SIEM system architecture is depicted in Figure 1 (IBM, 2010). The bottom of the figure shows the basic event collection and record retention capabilities. This retained data in the middle is then used for monitoring and correlation tasks. The top shows that the analyzed data can be reported in either security information or event driven reports.

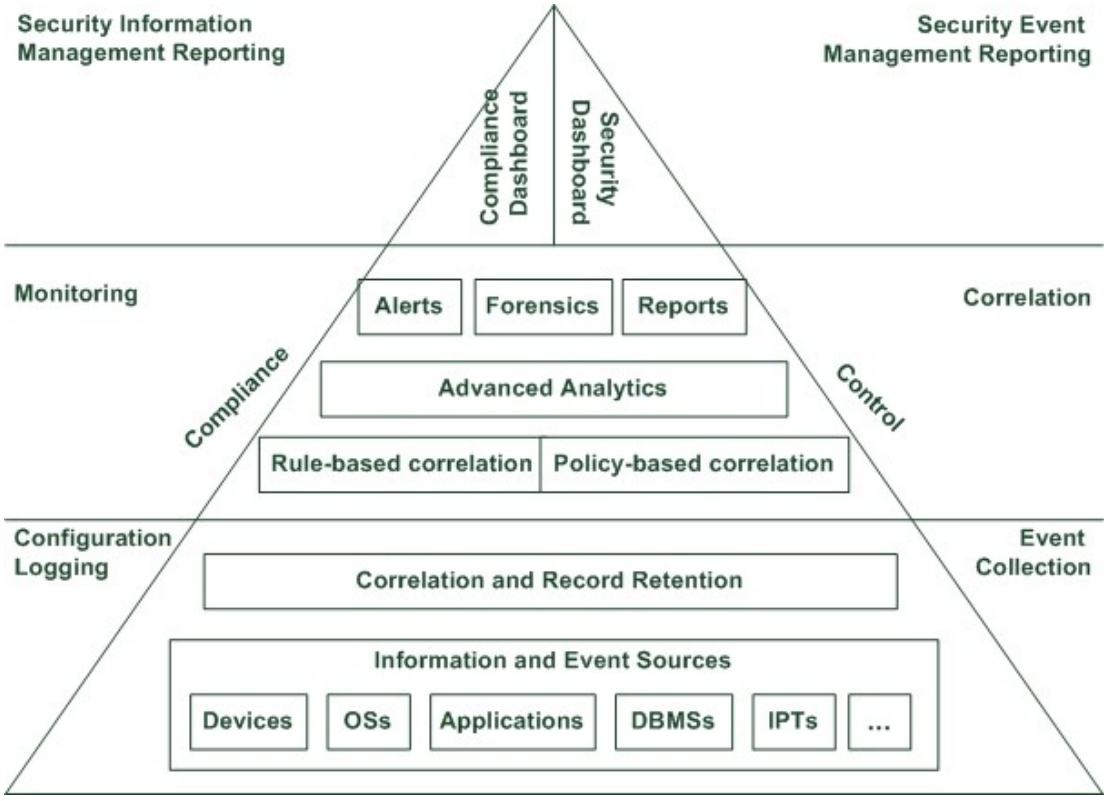


**Figure 1:** Typical SIEM system architecture

Two basic approaches are used in SIEM systems (Techtarget, 2014) (Scarfone, 2015):

1. Agentless, when the log-generating host directly transmits its logs to the SIEM or an intermediate logging server involved, such as a syslog server;
2. Agent-based with a software agent installed on each host that generates logs being responsible for extracting, processing and transmitting the data to the SIEM server.

Most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather IS-related events from IPTs, network equipment, end-user devices, servers, etc. The collectors forward events to a centralized management console, which performs inspections and flags anomalies.

SIEM systems can be rule-based (obvious disadvantages of this approach are time consuming of keeping up-to-date hundreds of rules, too many false positives and false negatives for constantly innovative attackers techniques), policy-based or have a statistical correlation engine to establish relationships between event log entries (IBM, 2010) (Miller, 2010).

All data processed by SIEM system should be protected itself as it contains very sensitive information needed for digital forensics and IS incident response.

# 3 SOCs and SIEM 1.0

While being integrated with another IPTs the SIEM systems can serve as a single window into the IS incidents for any organization. SIEM systems being used for constant event and user activity monitoring can detect and handle IS incidents through aggregation of large volumes of machine data in real time for IS risk management and essentially improve this automation. SIEM systems can also visualize IS threats to intranet's resources that may have otherwise been hidden. That is why they are considered as a core of SOCs. Let us define SOC as a centralized unit that deals with security issues on an organizational level plus a team primarily composed of security analysts (plus a few operators) organized to detect, analyze, respond to, report on, and prevent IS incidents in order to minimize IS risks (Miloslavskaya, 2014). IS risk is associated with the potential that IS threats will exploit vulnerabilities of an information asset/group of information assets and thereby cause harm to an organization. Risk is an effect of uncertainty on objectives (ISO27000, 2016).

Therefore, SIEM systems can help to achieve the following objectives in intranets' IS management (Miloslavskaya, 2014):

- To computerize activities for intranet's IS analysis and reporting in accordance with the applicable industry and international standards and regulations;
- To obtain information about the real state of the IS level throughout the organization's intranet and certain assets;
- To accelerate reaction to emerging of IS events and incidents and provides intranet's IS around the clock via automated response to IS events in accordance with the predetermined processing and correlation rules;
- To conduct a reasonable assessment of IS risks in the organization and timely eliminate or reduce IS risks based on this assessment;
- To detect differences and bring the intranet's assets and business processes in accordance with the internal IS policies, requirements of regulators and auditors;
- Formalize and implement effective decision-making in the field of IS;
- To eliminate the necessity to increase IS heard-count in accordance with increase in the number of IPTs, providing information on IS events;
- To reduce the cost of IS staff training as it becomes necessary to study only the interface of such a system instead of all the heterogeneous IPTs used in intranets.

The first-generation SIEM systems (SIEM 1.0) of the late 1990s, which have been widely used as an integral parts of SOCs, were log-centric and detect IS events through preset rules and information correlation techniques. The correlation was implemented mostly for IP addresses (today it is useless for the increasing number of mobile and remote users and the number of times a day they can change), although some systems could correlate ports and protocols usage and even users. Log files lack detail to understand what is truly happening at the moment. For example, logs may alert abnormally long query strings, unauthorized tunneling or encryption. But they cannot help to detect the specific client or malware activity with context, the use of unauthorized tools like Tor, SSL usage over unusual ports, non-standard network traffic, protocol anomalies, unauthorized connections and so on. According to

2015 Data Breach Investigation Report by Verizon 99 % of successful attacks went undiscovered by logs (Verizon, 2015). Another serious drawback of SIEM 1.0 is the relational DBs usage, which have the following limitations: little semantic richness and very simple structures, no support for recursion and inheritance, lack of processing/triggers, etc. All disadvantages of SIEM 1.0 (the paper lists only two of them) led to the need to develop the next generation of SIEM systems.

# 4 SICs and SIEM 2.0

New reality of more frequent and sophisticated attacks and «hacking as a service» makes intranets' break-in more professional, accessible and dangerously effective. Many organizations are beginning to realize that it is not enough to analyze IS-related data; they must also take action on it. They must oppose this properly designed and centralized IS management systems. This might be done semi-automatically or automatically to provide actionable insights and might include preventive maintenance, for instance, for monitoring their assets for issues based on past patterns or rules and trigger alerts that can improve security.

To implement such an approach and to automate to the limit all routine operations and IS incident response that do not require expert's decision-making is an urgent need for any modern organization to set up IS management center dealing with these challenges and being more advanced than a traditional SOC. So called SIC with an integrated attacks defense architecture provides full visibility and control and context-driven security intelligence in one place to temporarily deal with network-level and more important higher-level IS events. Implementing SICs, organizations have a holistic in-depth view of their intranet's «IS health» and they are capable not only to detect and recognize attacks, but also to effectively address IS threats before they cause harm and prevent IS incidents, constantly gathering and processing knowledge about network attacks. With in-house private SIC, based on the second-generation SIEM system, the organization can get a personalized network security management.

The second-generation SIEM systems (SIEM 2.0) started in the late 2000's perform behavioral and contextual analysis and implement the following basic functions:

1. Real-time detection and centralized collection of information about IS events from all distributed heterogeneous intranet's sources: IPTs (software and hardware), network devices, applications, DBs, configuration files, etc.;
2. Monitoring of user activity and application in a certain context;
3. Collected information processing (including its filtering, aggregation, normalization, correlation, etc.) in a particular context, given previous and current user's and application's activity and accumulated statistics;
4. Tracking the entire lifecycle of each IS incident – analysis and automatic execution of certain actions in response to IS events classified as IS incidents;
5. Automated generation of reports and recommendations to handle IS incidents and events (including tracking of their solution status) and summary reports on intranet's IS level;
6. Usage of big data technologies with in-memory and in-database analytics, massive parallel programming and so on (instead of relational DBs) for scalable IS analytics.

Having all these in SICs, the organizations get the following key advantages:

- Alignment of IS risk management with business needs, based on predefined meaningful IS metrics and 24x7 security coverage, combining local monitoring observations, continuously recorded history, external SI and internal threat intelligence, cross-channel visibility in a single view and entity link analysis to reveal hidden relationships and

suspicious associations among users, accounts or other entities early in their life cycles in one place without requiring full-time staffing;

- A holistic proactive and predictive approach with behavioral-based cross-correlation and advanced context-based (not event-by-event) analytics, meaning that an organization is looking at every aspect of its IS threat management in relation to every other aspect, views IS as more than a matter of mitigating IS risk by identifying and patching vulnerabilities on network assets, as well as considering IS threat capabilities and motives against intranet's assets;
- More focused approach concentrates its resources on concrete network security threats with prioritizing the redundant multiple layers of IS that constitute borrowed from the military affairs «Defense-in-Depth» strategies and strategically orchestrating these layers.

# 5 Conclusion

At present even SIC's idea does not keep pace with the increasing number of sophisticated IS threats in highly heterogeneous connected world. The next evolutionary step towards creation of more effective IS management structure for securing organizations' IT assets is expected as never before. In our opinion, this progressive structure should unite all benefits of SIC with many years experience of network operations management, implemented in NOCs – Network Operations Centers. Our future work is aimed at their design.

# 6 Acknowledgement

This work was supported by the MEPhI Academic Excellence Project (agreement with the Ministry of Education and Science of the Russian Federation of August 27, 2013, project no. 02.a03.21.0005).

# References

ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary.

IBM Corporation (2010). IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager. 2nd edition. URL: http://www.redbooks.ibm.com/abstracts/sg247530.html?Open (access date 05/03/2017).

Techtarget (2014). Security information and event management (SIEM). URL: http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM (access date 05/03/2017).

Scarfone, K. (2015). Introduction to SIEM services and products. URL: http://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products (access date 05/03/2017).

Miller, D., Harris, S., Harper, A., VanDyke, S. (2010). "Security Information and Event Management (SIEM) Implementation". McGraw-Hill. 2010. 464 p.

Miloslavskaya, N.G., Senatorov, M.Y., Tolstoy, A.I. (2014). "Information Security Management Issues" Series. In 5 volumes. Volume 3: Information Security Incident and Business Continuity Management. Moscow: Goriachaja linia-Telecom. 2014. 2nd edition. 170 p. (In Russian)

Verizon (2015). Data Breach Investigations Report. URL: http://www.verizonenterprise.com/DBIR/2015/ (access date 05/03/2017).