An Event Management System For Detecting Brute Force Attack

Adebukola S. Onashoga
Department of Computer Science,
Federal University of Agriculture, Abeokuta.
onashogasa@funaab.edu.ng

Oreolorun Omolara Odewale
Department of Computer Science,
Ibadan City Polytechnic, Ibadan.
omolaraodewale@gmail.com

Oluwatoyin E. Adeleye
Computer Technology Department,
Yaba College of Technology, Lagos.
thelordsdoing_14@yahoo.com

Adedoyin A.Bababiola
Department of Computer Science,
Federal University of Agriculture, Abeokuta.
doyinbabs42@gmail.com

Abstract— *Event logs are important forensic tools for investigating an organization's security posture. A key challenge facing Information Security practitioners today is the timely and effective collection, collation and analyses of the security events generated from a wide source of network systems, security mechanisms, systems and applications deployed across a modern business. Through intelligent event management, security teams can identify vulnerabilities in their infrastructure, as well as enumerate, alert and report on attempts to exploit these vulnerabilities. In this work, a Real-time Intelligent Monitoring Architecture (RIMA) was developed for efficient Security Event Management System suitable for the detection of brute force attack. RIMA consists of five phases namely data collection, normalization, storage, correlation, and monitoring. A multiple matching algorithm (MMA) was developed for RIMA for efficient event classification. For the implementation of RIMA, a web based SEM system was developed to help us detect brute force attacks on a target windows machine. To achieve this, we collected the security event audit logs from the target machine and fed it into the RIMA database, after which the data is being normalized and correlated to detect the brute force attacks. The report of the analysis was generated and displayed on the RIMA user interface. The results showed a system that can be used to detect brute force attack efficiently*.

I. INTRODUCTION

Operating systems, devices and applications all generate some sort of logs that contain system-specific events, alerts and notifications (Greg et al, 2008). With the continuous improvement of modern server and application software, logging has become a staple of the IT management and monitoring process. And, until recently, this is primarily as a result of the ease of generating log data — not in using it.

Event logs also provide historical information that can help track down system and security bugs and problems. The event-logging service controls whether events are easily

tracked on Windows 2000 systems. When this service is started, we can track user actions and system resource usage events with the following event logs:

- Application Log records events logged by applications, such as the failure of MS SQL to access a certain database.
- Directory Service records events logged by an Active Directory and its related services
- DNS Server records DNS queries, responses, and other DNS activities.
- File Replication Service Records file replication activities on the system.
- Security Log Records events you've set for auditing with local or global group policies.
- System Log records events logged by the operating system itself or its components, such as the failure of a service to start at boot up.

Security event management (SEM) is the process of identifying, collecting, monitoring and reporting security-related events in a software, system or IT environment. SEM enables the documentation and evaluation of events, and helps security/system administrators to analyze, and manage the information security architecture, policies and procedures (Techopedia).

Security Event Management was pioneered by a small company called E-Security in 1999 (ZDNet, 2006), and are still evolving rapidly. The main feature of a Security Event Management tool is the ability to analyze the collected logs to highlight events or behaviors of interest, for instance, an Administrator or Super User logon, outside of normal working hours.

With the evolution of faster and more efficient password cracking tools, brute force attacks remain some of the most common methods for compromising organizational network. To monitor and check for unauthorized access in real-time, SEM technology can be utilized to detect brute force patterns on the network. This will involve log collection from all the platforms that require authentication.

The rest of this paper is organized as follows: Literature review was presented in section II. The RIMA architecture was presented in section III. The RIMA system was implemented in section IV. And the paper is concluded in section V.

II. RELATED WORK

Granadillo et al. [24] proposed two novel alert correlation approaches for efficient handling and management of security incidents. It was assumed that as the number of security incidents, and thus the diversity of alerts received by SIEMs increases, the need for appropriate treatment of these alerts become essential. The research concentrated on providing information about the attacker's behavior and the defender's capability in reacting to detected attacks. The first novel alert correlation approach proposed is based on policy enforcement and defender capability models; and the second is based on information security indicators. The aim is to enrich the current state of the art in alert correlation techniques.

Hershey *et al.* [25] in their work proposed a new framework for monitoring and managing cyber security events in complex systems in order to protect both the systems and data they carry against cyber-attacks while, at the same time, providing high quality end-to-end services that meet service level agreements and help ensure mission success. The research concentrated on procedures, methods, and policies to provide an effective enterprise cyber security monitoring and management solution.

Suarez-Tangil *et al.* [26] in another work applied Artificial Immune Systems (AISs) to solve the semi-automatic generation of event correlation rules. It was assumed that even though there is a vast number of novel initiatives and contributions in providing intelligence in this research field, there are still many problems that need be solved. In particular, event correlation is currently emerging as an essential field to be optimized especially due to the widespread adoption of botnets to launch attacks.

AlSabbagh *et al.* [27] presented a socio-technical framework for integrating a security risk escalation maturity model into a security information and event management system. The objective of the framework is to develop the foundations for the next generation socio-technical security information and event management syste`ms (ST-SIEMs) enabling socio-technical security operations centers (ST-SOCs). The primary benefit of the socio-technical framework is twofold: supporting organizations in overcoming the identified limitations in their security risk escalation maturity, and supporting SOCs in overcoming the limitations of their SIEMs.

III. METHODOLOGY

A SEM can be compared to a complex machine in that a SEM has several moving parts, each performing a specific job, that need to work properly together or else the entire system will fail.

There are variations on the standard SEM, with additional specific parts. The RIMA proposed in this work has five separate components. These individual components are the data/log collection, parsing/normalization of the logs, the rule engine, log storage, and event monitoring and retrieval.

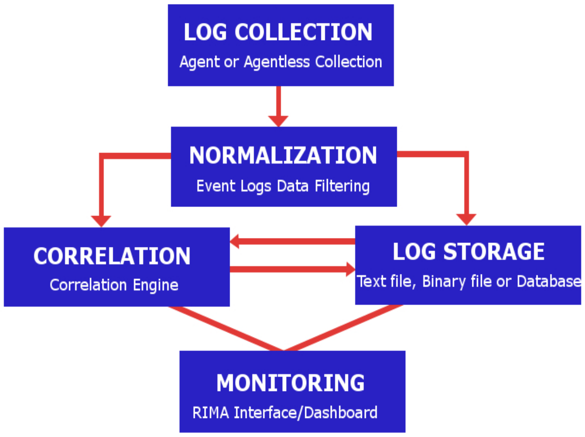


Fig. 1. RIMA Archictecture

A. *Data Collection*

The first part of a RIMA is data collection that feeds information into the RIMA. To begin data collection, data is retrieved from the source device and then store and process in RIMA. The source device can be an actual device on your network, such as a router, switch, or some type of server, but it can also be logs from an application or just about any other data that you can acquire. Without the source device and the information that these devices generate, RIMA is just a nice application that does nothing.

RIMA uses several techniques to collect log events from connected devices. Each of these methods has their advantages.

- Collection Using Agents

  Agents are processes running on a device. These processes can collect log events from multiple sources such as multiple applications and normalize events so they can be compared more easily. They are sent over a secure line to the Collector.

- Agentless Collection

  Agentless collection involves all methods in which the device sends the log events to a Collector or where the Collector retrieves all events from a network share, – drive or another (protected) source. Instead of an agent the collector will take on most of the normalization and categorization tasks.

  On a windows target machine, agentless collection approach can be utilized to collect security event logs. We can do this manually by exporting the logs from the windows event viewer or automatically using PowerShell. These logs are then fed into the RIMA central database for correlation and analysis to detect brute force attack on that machine.

B. Normalization

Now that the logs from the machines in your environment are being forwarded to the SEM, what happens next? At this point, the logs are all still in their native format so you have not really gained anything, other than a centralized repository for your logs. What needs to happen in order to make these logs useful in the SEM is to reformat them into a single standard format that is usable by the SEM. The act of changing all these different types of logs into a single format is called normalization.

Each type of SEM will handle the act of normalization in different ways, but the end result is to have all the logs, no matter what type of device or manufacturer, look the same in the SEM.

In RIMA, we utilized a simple yet intelligent normalization technique to normalize the security event audit logs collected from the windows target machine into a single easy to read format.

RIMA Normalization/Filtering Algorithm for analyzing Windows Security Events Logs to detect brute force attacks.

```
1. Validate the CSV event logs file before uploading
2. Open the uploaded CSV event logs file link
3. Count the number of rows
4. If the rows are more than 1000, break it into batches of 1000 for processing
5. Loop through each event records to normalize the event logs
     i.   If the event code is 4624, set the EventType to "logon success"
     ii.  If the event code is 4625, set the EventType to "logon failure"
     iii. Event codes with 4624 and 4625 signifies a Windows Security Event Audit Log hence a Windows OS to be set as the event source
     iv.  After normalization, insert the records into the RIMA Database event table
     v.   Get the insert_id after the very first insert to be set as the firstEventID for the event logs
     vi.  To set lastEventID, get the insert_id which will updated after the very first insert
6. End loop
```

C. Correlation

Correlation is very important in SEM and a vital piece of RIMA. It greatly reduces the number of false positives. It is used to reduce the (possible huge) number of events down to a limited number of alarms and events using various methods of correlation.

- Correlation engine

  What the correlation engine does is to match multiple standard events from different sources into a single correlated event. Correlation of standard events into a correlated event is done in order to simplify incident response procedures for your environment, by showing a single event that is triggered off of multiple events coming from various source devices.

A multiple matching algorithm (MMA) developed for the correlation engine for analyzing Windows Security Events

Logs to detect brute force attacks. Below is the MMA set-based pseudo code.

```
1. Select eventDate, count(EventType) as
   failed_logon_count over Event_source_ip of the target
   machine/server from the RIMA Database event table
2. Restrict the result of the select for only rows between
   two EventIDs given
3. Restrict the result of the select to EventType of "logon
   failure"
4. Group the result of the select by event date into every 5
   mins' interval
5. Group the result of the select by EventType of "logon
   failure"
6. Loop through the results,
     i.   If failed_logon_count is more than 10, it may
          signify a brute force attack
     ii.  Add 5 mins' interval to the eventDate (starting
          date of the brute force attack period) to get the
          exact timeframe when the brute force attack
          occurred
     iii. Print the failed_logon_count as well as the
          timeframe when the brute force attack occurred
7. End loop
```

D. *Log Storage*

All events received by the RIMA environment are stored in a database. In order to work with the volumes of logs that come into the SEM, we need a way to store them for retention purposes and historical queries. There are typically three ways that SEMs can utilize to store its logs: in a database, a flat text file, or a binary file.

- Database

  Storing logs in a database is the way most SEMs store their logs. The database is usually a standard database platform such as Oracle, MySQL, Microsoft SQL, or one of the other large database applications being used in the enterprise. This method allows for fairly easy interaction and retrieval of the stored data because the database calls are part of the database application. Performance should also be fairly good when accessing the logs in the database, depending on what hardware the database is running on, but the database application should be optimized to run with the SEM.

E. *Real-time Monitoring And Reporting*

The final stage in the anatomy of a SEM is the method of interacting with the logs stored in your SEM. Once we have all the logs in the SEM and the events have been processed, we need a way to do something useful with the information—otherwise the logs are just in the SEM for storage purposes. A SEM will have a dashboard/interface/management console, which is usually web-based, running on the SEM server that has been set up to be such an end point.

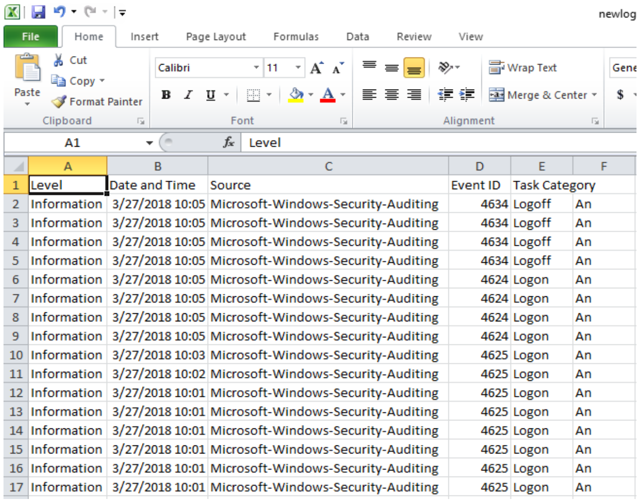
This interface into the actual SEM application will allow the incident handlers or system engineers a unique view into the IT environment. Normally, in order to view the information that the SEM gathers, incident handlers or engineers would have to go to the different devices and view the logs in their native formats. The SEM makes viewing and analyzing all these different logs much easier because the SEM normalizes the data.

The RIMA dashboard provides a general overview. It provides tools for analysis of security events and raw log files. This interface will allow one to interact with the data stored in the RIMA.

IV. EVALUATION AND RESULTS

Evaluation experiment using data collected from the source device was conducted.

The security event manager normalization and correlation engine using a sample security event logon data collected/exported from a windows machine event viewer as show below;

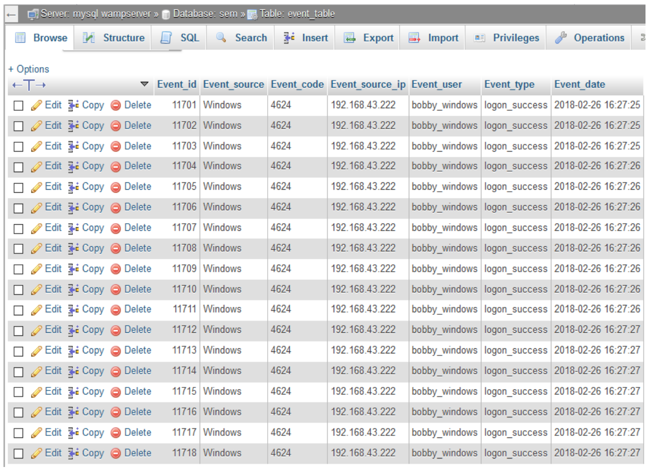


	A	B	C	D	E	F
1	Level	Date and Time	Source	Event ID	Task Category	
2	Information	3/27/2018 10:05	Microsoft-Windows-Security-Auditing	4634	Logoff	An
3	Information	3/27/2018 10:05	Microsoft-Windows-Security-Auditing	4634	Logoff	An
4	Information	3/27/2018 10:05	Microsoft-Windows-Security-Auditing	4634	Logoff	An
5	Information	3/27/2018 10:05	Microsoft-Windows-Security-Auditing	4634	Logoff	An
6	Information	3/27/2018 10:05	Microsoft-Windows-Security-Auditing	4624	Logon	An
7	Information	3/27/2018 10:05	Microsoft-Windows-Security-Auditing	4624	Logon	An
8	Information	3/27/2018 10:05	Microsoft-Windows-Security-Auditing	4624	Logon	An
9	Information	3/27/2018 10:05	Microsoft-Windows-Security-Auditing	4624	Logon	An
10	Information	3/27/2018 10:03	Microsoft-Windows-Security-Auditing	4625	Logon	An
11	Information	3/27/2018 10:02	Microsoft-Windows-Security-Auditing	4625	Logon	An
12	Information	3/27/2018 10:01	Microsoft-Windows-Security-Auditing	4625	Logon	An
13	Information	3/27/2018 10:01	Microsoft-Windows-Security-Auditing	4625	Logon	An
14	Information	3/27/2018 10:01	Microsoft-Windows-Security-Auditing	4625	Logon	An
15	Information	3/27/2018 10:01	Microsoft-Windows-Security-Auditing	4625	Logon	An
16	Information	3/27/2018 10:01	Microsoft-Windows-Security-Auditing	4625	Logon	An
17	Information	3/27/2018 10:01	Microsoft-Windows-Security-Auditing	4625	Logon	An

Fig. 2. Windows security event logs data

The goal here is to normalize the event logs, save it to the SEM database, analyze the events, correlate it, and then generate a report.

Below is an overview of the RIMA MYSQL database after the data has been saved or fed into the database.



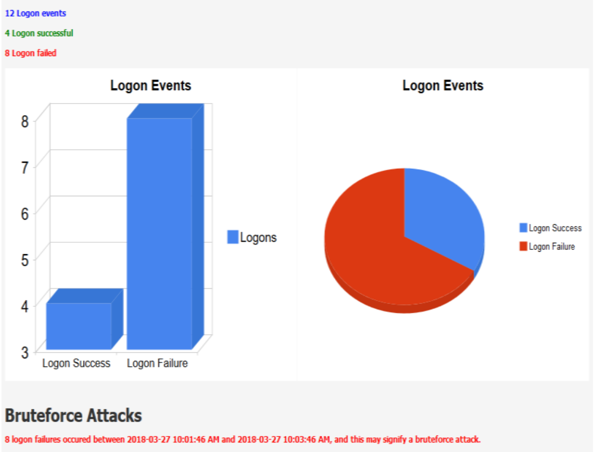
	Event_id	Event_source	Event_code	Event_source_ip	Event_user	Event_type	Event_date
□ Edit Copy Delete	11701	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:25
□ Edit Copy Delete	11702	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:25
□ Edit Copy Delete	11703	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:25
□ Edit Copy Delete	11704	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:26
□ Edit Copy Delete	11705	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:26
□ Edit Copy Delete	11706	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:26
□ Edit Copy Delete	11707	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:26
□ Edit Copy Delete	11708	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:26
□ Edit Copy Delete	11709	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:26
□ Edit Copy Delete	11710	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:26
□ Edit Copy Delete	11711	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:26
□ Edit Copy Delete	11712	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:27
□ Edit Copy Delete	11713	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:27
□ Edit Copy Delete	11714	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:27
□ Edit Copy Delete	11715	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:27
□ Edit Copy Delete	11716	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:27
□ Edit Copy Delete	11717	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:27
□ Edit Copy Delete	11718	Windows	4624	192.168.43.222	bobby_windows	logon_success	2018-02-26 16:27:27

Fig. 3. RIMA MYSQL Database Event Log Table

Looking at the above data in the table/Fig 1, it shows multiple logon events over a 5 minutes' period. We can see the login failures (4625) and login successes (4624). If we look closely, we can see a pattern of multiple logon failures times, and then all of the sudden we see a successful login. This could possibly be a brute-force attempt against the target server or machine, but unless you have a really good memory, you may have forgotten that the first event happened.

When a hacker is trying to brute-force your server, they are attempting to steal login credentials – both usernames and passwords. Sometimes, they steal this in pre-compiled lists, while in other times; they generate this on the go. Once they have these pieces of information, they will try to use them to launch attacks on your server. In many cases, they automate these attacks. The ultimate goal of these attackers is to find a set of login credentials that will allow them successful entry into your server.

We will analyze this data using the RIMA system to generate the results as shown below;


12 Logon events

4 Logon successful

8 Logon failed

Bruteforce Attacks

8 logon failures occured between 2018-03-27 10:01:46 AM and 2018-03-27 10:03:46 AM, and this may signify a bruteforce attack.

Fig. 4. SEM Brute Force Attacks Reporting

V. CONCLUSION

A correctly implemented security event management solution will improve the effectiveness of security monitoring and incident response functions. Analysts will spend less time monitoring consoles and reviewing security logs because this function is automated by the SEM system. Senior analysts can build expert know-how into the rule system to improve the quality of alerts for all analysts, and reduce cases of false positives.

Having all security events collected into one central database is a key benefit of a SEM system. This information is very valuable for security analysts, incident response teams, and other IT teams. Reports and security metrics can be generated for managers and data mining tools can uncover interesting information from the data.

The benefits do come at a cost, however, and it will take several months to start realizing the benefit of implementing an SEM system. In addition to the cost of developing a solution, perhaps two of the most resource intensive efforts are integrating security event sources into the system and performing tuning of the rule system. When implementing the SEM system, it is important to ensure that all data of importance is collected and available within the database. If the data is not available, then it cannot be queried or displayed and it is frustrating to run a query or report only to find that a needed field is not available because it has not been collected. The value of the SEM system then is only as good as the information it contains.

Vendors of commercial SEM solutions offer professional assistance, but it is beneficial for analysts to be involved in the implementation process to understand the workings of the whole system. Analysts will also need training in the use and administrator of the system.

It will be of immense benefit if further research would be conducted to further look into other platform of this system. It will be of great advantage if the research could be extended to an agentless solution that will handle all the log collection, normalization, correlation and analysis.

Security Information and event management technologies saw some consolidation in 2006. EMC acquired Network Intelligence, Novell acquired eSecurity, IBM acquired Micromuse, which had acquired Guardednet, and IBM also acquired Consul. Today there are lots of large, established broad-scoped vendors and point solution vendors trying to capture the roughly $300 million in revenue the SIEM market was estimated to be in 2006. How is this sustainable? What will happen to the market in the next 2-3 years? Today we are now entering the advanced stage of SIEM technology. SIM (Security Information Management) and SEM (Security Event Management), is now advancing into a "security big data analytics" platform.

Future work in SEM will lean towards how to efficiently provide more accurate analysis from big data and how to increase the fidelity of the data a SIEM collects. Full packet capture will be the key capability of the future SIEM system, which means big data will be at the foundation of any effective SIEM product.

The SIEM market will begin to diverge into a SEM market driven by network and systems oriented tools focused on the threat, configuration and policy compliance needs, pushed by vendors such as Cisco Symantec, and NetIQ and a SIM market driven by user-centric auditing and monitoring, integrations with IAM systems, focused on regulatory compliance initiatives, pushed by vendors such as CA, IBM, and Novell.

REFERENCES

[1] B. AlSabbagh, and S. Kowalski. "A Framework and Prototype for A Socio-Technical Security Information and Event Management System (ST-SIEM)". Department of Computer Science, University Carlos III of Madrid, Avda. Universidad 30, 28911, Spain, 2016.

[2] A. Vault. Open Source Community. (2012). “OSSIM Management Server”. Retrieved January 10, 2018, http://goo.gl/olg4F

[3] Business Rules Group. Business Rules Manifesto. Retrieved January 2018, http://goo.gl/GZ1OE

[4] E. de Bueger. “White paper: Security Information & Event Management”, Technical report, Kahuna Group, January 2012.

[5] J. M. Butler. (2007). “Benchmarking security information event management (SIEM)”. Retrieved January 10, 2018, http://goo.gl/yMvq5

[6] A. Chuvakin. (2012). “Practical strategies to compliance and security with SIEM”. Retrieved January 10, 2018, http://goo.gl/kifj2

[7] A. Chuvakin. (2010). “The complete guide to log and event management”. Retrieved January 10, 2018, http://goo.gl/0lr7f

[8] A. Chuvakin. (2011). “Leveraging compliance for security with SIEM and log management”. Retrieved January 10, 2018, http://goo.gl/m3lLQ

[9] Dr. Dobb. (2007). SIEM: A Market Snapshot. Retrieved January 10, 2018, http://goo.gl/Blc7u

elQnetworks, Web. (2013) “elQnetworks Survey Reveals Organizations Are Suffering from SIEM Deployments”, Retrieved January 10, 2018, http://www.eiqnetworks.com/news-events/press-releases?pr=eiqnetworks-surveyreveals-organizations-are-suffering-from-siem-deployments

[10] G. G. Granadillo, M. El-Barbori, and H. Debar. "New Types of Alert Correlation for Security Information and Event Management Systems". Inst. Mines Telecom, Telecom SudParis, Evry, France, 2016.

[11] D.F. Greenberg and J.B. Roush. “The effectiveness of an electronic security management system in a privately-owned apartment complex”. Sociology Department, New York University, 2008.

[12] Greg et al, (2008). "Are SIEM and log management the same thing?" Network World, 2008

[13] J. Hernandes. “Security information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives”, ISACA, 2010.

[14] P. C. Hershey, C. B. Silio. "Monitoring and management approach for cyber security events over complex systems". Raytheon Intelligence and Information Systems, 22110 Pacific Blvd, Dulles, VA 20166, USA, Department of Electrical and Computer Engineering, University of Maryland, College Park, 20742-3285, USA, 2011.

[15] N. Hutton, (1995), “Preparing for Security Event Management”. Retrieved January 10, 2018, http://www.360is.com/white-papers/preparing-for-security-event-management.html

[16] Hewlett Packard. (2012). “HP ArcSight express: powered by the CORR-engine”. Retrieved January 10, 2018, http://goo.gl/cZnBG

[17] K. D. Mitnick, and W. L. Simon. “The art of intrusion, the real stories behind the exploits of hackers, intruders and deceivers”. Indianapolis, IN: Wiley, 2006.

[18] M. Nicolett. “How to implement SIEM technology”. Technical report, Gartner Research, November 2009.

[19] RSA. (2011). “An integrated approach to risk, operations and incident management”. Retrieved January 10, 2018, http://www.rsa.com/products/sms/sb/11508_ h9010-iaroim-sb-0811.pdf.

[20] E. Skoudis, and T. Liston. “Counter Hack Reloaded: A step - by - by step guide to computer attacks and effective defenses”. Upper Saddle River, NJ: Pearson, 2006

[21] S. David. (2006). "A Practical Application of SIM/SEM/SIEM, Automating Threat Identification" (PDF). SANS Institute. p. 3. Retrieved January 10, 2018.

[22] G. Suarez-Tangil, E. Palomar, S. Pastrana, A. Ribagorda. "Artificial immunity-based correlation system". Department of Computer Science, University Carlos III of Madrid, Avda. Universidad 30, 28911, Spain, 2011.

[23] Techopedia, “Security event management” Retrieved January 10, 2018, https://www.techopedia.com/definition/25763/security-event-management