



*The World's Largest Open Access Agricultural & Applied Economics Digital Library*

**This document is discoverable and free to researchers across the globe due to the work of AgEcon Search.**

**Help ensure our sustainability.**

Give to AgEcon Search

AgEcon Search

<http://ageconsearch.umn.edu>

[aesearch@umn.edu](mailto:aesearch@umn.edu)

*Papers downloaded from **AgEcon Search** may be used for non-commercial purposes and personal study only. No other use, including posting to another Internet site, is permitted without permission from the copyright owner (not AgEcon Search), or as allowed under the provisions of Fair Use, U.S. Copyright Act, Title 17 U.S.C.*

*No endorsement of AgEcon Search or its fundraising activities by the author(s) of the following work or their employer(s) is intended or implied.*

**Pál Michelberger**<sup>1</sup>  
Óbuda University,  
Keleti Faculty of Business and Management  
**Sándor Dombora**<sup>2</sup>  
PhD Student, Óbuda University,  
Doctoral School on Safety and Security Sciences

SCIENTIFIC REVIEW ARTICLE  
doi:10.5937/ekonomika1601125M  
Received: November 15, 2015  
Accepted: February 20, 2016

## A POSSIBLE TOOL FOR DEVELOPMENT OF INFORMATION SECURITY - SIEM SYSTEM

### Abstract

*The implementation of information security for governmental institutions is regulated by laws, which specify the development of complex regulation environment and implementation of information security solutions. The implementing regulation emphasizes the minimal user access rights principle, which means employees should be provided with necessary and sufficient rights to do their jobs, prescribes the implementation of a control system which limits user activities to the execution of their tasks, requires security analysis of information systems' log files of organizations handling large volume of personal data. Considering that the weakest point is the user, the most important aspect of log file processing is user activity analysis, building user profiles, identifying unusual events based on these and analyse them based on the data available about users for the organization. The paper discusses the goal, role, possibility, the importance and limitations of building user profiles instantly by analysing log files, considering efficiency, and all-inclusiveness with minimization of false alarms and administration tasks based on information available electronically about employees. By the end of the paper a cost-effective model is presented for automated user activity and profile analysis.*

**Key words:** SIEM, user activity analysis, user's profile, security awareness

**JEL classification:** M15, M59

## МОГУЋИ ИНСТРУМЕНТ РАЗВОЈА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ – СИЕМ СИСТЕМ

### Апстракт

*Обезбеђење информационе безбедности државних институција регулисано је законом, којим се утврђује развој комплексног законодавног оквира и имплементација безбедоносних решења. Регулатива посебан акценат ставља на принцип минималног приступа корисника, којим се запосленима пружају само неопходна овлашћења како би обављали свој посао. Са друге стране, регулатива прописује употребу система контроле који лимитира активности корисника*

<sup>1</sup> michelberger.pal@kgk.uni-obuda.hu

<sup>2</sup> dombora.sandor@kvk.uni-obuda.hu

у обављању њихових задатака и захтева анализу безбедности датотека информационог система које садрже велике количине личних података. Имајући у виду да је најслабија карика корисник, најзначајнији аспект обраде датотека је анализа активности корисника, израда профила корисника, идентификовање необичних појава и на основу тога анализа доступних података о корисницима организације. У раду се сагледава циљ, улога, могућности, значај и ограничења за израду корисничких профила путем анализе датотека, имајући у виду њихову ефикасност и свеобухватност са минимумом лажних узбуна и административних задатака на основу електронски доступних података о запосленима. На крају рада је дат модел исплативости за аутоматске активности корисника и анализу профила.

**Кључне речи:**СИЕМ, корисник анализа активности, профил корисника, безбедност свести.

## 1. Introduction

Several international research studies conducted by consulting companies confirm that users and administrators, employees and managers represent the biggest information security risk (Ernst & Young, 2014), (PwC, 2015), (A Frost & Sullivan Market Study in Partnership with ISC2, 2013), etc. Furthermore the risk is boosted by the evolution of information technology. We should also consider the impact of social media sites and the use of private mobile assets for business purpose.

One way of handling the risk of the human factor is the traditional identity, user rights and role management regulation and enhancement of it with the new type of information security assets. The access of confidential data stored on file servers of organizations (companies) can be queried regularly (File Audit). Naturally the prerequisite for this is the classification of files in protected security classes.

By building user profiles during the operation and administration of information systems we can perform continuous “monitoring”, investigate the user’s motivation, information security knowledge, attitude and awareness in cases of unusual behaviour. This means a preventive information security activity, which cannot be considered paranoia by the chief information security officer. It is easy to filter out the unusual user behaviour events from the standard and routine working activity using the log-entries database.

By using a modern SIEM (Security Information and Event Management) system, we can get an overall view of the information security activity of the organization (Miller et al., 2014). Such a special IT system gathers and stores the events related to information security regarding users, data flow, network, and security assets (e.g. firewalls, antivirus, intrusion detectors, etc.). The security analysis of events means comparison to the “usual” operation. By gathering, aggregating and analysing the log data from different sources, the intentional and unintentional damages caused by security events can easily be localized.

## 2. Paradigm shifts regarding information and IT security risk analysis

By now organizations employ user restrictions, strictly regulating and control based business processes supporting an information security systems approach. This all-inclusive “protection” (event monitoring 24 hours a day, management of different overlapping security technologies, log analysis, operations) can be regarded as less efficient because of changing threats.

Nowadays, the information security services provide several effective possibilities (Kim & Solomon, 2013):

- Internal firewall management;
- Automated journal and log analysis (data access monitoring);
- Vulnerability assessment (discovery, classification, analysis, risk assessment of assets in internal network, fixing and verifying vulnerabilities);
- Automatic security assessment of Internet application;
- Verification of Wi-Fi security;
- Controlling network access (user authentication, handling, inadequate users, exclusion of unauthorized network end points);
- Intrusion signalling;
- Emphasized handling of sensitive data after classification;
- Event management (infrastructure, log analysis of assets and applications).

This means continuous monitoring of the users' behaviour and filtering as well as dedicated investigation of the unusual activities using mathematical methods (distribution analysis, pattern matching, and text analysis). Alerting the staff happens after ranking the log entries by risk, so they can focus on the most important and risky events. The efficiency of security measures can be increased by reasonable restriction of the scope of risk assessment territory.

During logging in it is recorded: what and when changed, who executed and from which access point was started the transaction as well as whether or not the change was allowed/approved.

The information systems security as well as the information security of organizations should be assessed from several points of view. The efficiency of SIEM systems requires alignment of the information security measures (policy) of the company, IT assets and company processes.

In information protection, we can distinguish security levels (Park et al., 2008):

- Information technology infrastructure security (configuration management, hardware, software and network protection);
- Information handling (record, change, delete, and inquire respectively);
- Business processes (process control, workflow, IT support of products and services, customer service activities);
- Organization (information security strategy, risk management, organization structure, management style, company culture, support of management activities);

This “holistic” access control system approach is a good example. We can find activities related to this on all four levels:

- IT level – user authentication;
- Information handling – providing minimal user access rights to data necessary for execution of work activities;
- Process level – splitting critical processes, entitlements attached to persons and locations;
- Organization level – risk avoidance, development of access groups and regulation of access control system and continuous monitoring.

Maria Karyda et al. (2005) developed a general operational security model for information systems in which besides the security level plays a role:

- The change management (in organization structure, organizational behaviour, processes and information technology) – as *information-content*.
- The external and internal contacts, *relationships* (economic, legal, political and social factors, industrial competition, supplier circumstances, internal elements of organizational culture).
- The cultural and power viewpoint approach of the business processes (presence of security needs in organizational culture, and enforcement of power in information security policy).

### 3. Entitlement, role and identity management

The transaction management and management information systems (e.g. ERP, CRM, EAM) support, model and several times optimize the value generation and support process execution of the company. The employees (the users) in their scope of activities execute “basic” tasks by using information technology resources. They record, edit, query, maybe delete data, to ensure information – as a resource - availability for the different levels of decision makers.

In the case of many users and several heterogeneous information technology based information systems, the identification and system access monitoring may become completely chaotic. Gaps and/or overlapping may arise in authorization and authentication. User rights are not always established based on actual tasks or scope of activities. Rather established customs or organization traditions are taken into account. Overlapping user access management may evolve for the independent information systems of the organization. Several times the user access management administration is done after change completion (employee transfer, exit, new process implementation, outsourcing, etc.).

The solution could be the development of a role based organizational structure and process analysis, which can be combined with identity management of users with role association.

The employee who executes the company processes uses the information technology assets of the company. Naturally the user does not need all IT assets and all the stored data of the company. The *access rights* limit the user’s interaction, optimally to the information management tasks needed by his/her scope of activities. The basis for access rights should be the business processes, their scope, organizational structure and IT infrastructure. The information security risks (loss or unnecessary access of valuable

company information) are related. The organization and individual knowledge, the company culture, and the responsibility accompanying the scope of activity affect the development of the concrete authorization system.

The access rights (deliverable, implementable, adjustable, controllable, rejectable, interruptible and removable) are registrable and should be registered. It is very important to obtain the approval of the workplace manager and the responsible information security officer. In simple cases the employee is provided with a username (login) and a password. In the case of higher security levels, needs can be complemented or replaced with biometric “identifiers” (e.g. fingerprint, iris, earlobe, etc.) or complemented with hardware assets. These are associated with information systems, business application modules, menus, screens, input fields, and database query possibilities regarding business processes and company goals. The access rights can be bounded to operational place and time.

Regarding their scope of activities, sometimes the users should have access to several information systems. This means that they should “prove” their access right several times. This can happen by using owned assets (You have ...) suitable for identification (chip and magnetic cards, hardware keys).

In the case of a large number of systems, the knowledge base (You know...) identification is hard to implement, just think of a private person and how many passwords they have. Furthermore, these should be changed from time to time because of security reasons.

Simplicity might be achieved through the use of biometric elements (fingerprint, handprint, iris, vein, DNS) for identification (You are ...). Their usage raises a human rights issue. In every case, employers cannot require their use by employees.

Security becomes complete with the development of adequate roles and the connected role entitled systems.

In case of medium and large enterprise companies with multiple premises, executing “standardized” processes with role implementation is worth considering. Users in the same role get the same access rights. The role might be connected to several applications. In this way the setup of user access rights may be automated and mass changes can be performed easily once. The necessary access rights may be filtered and the number of individual access rights can be reduced to a minimum. Thus, the number of roles will be smaller than the number of users.

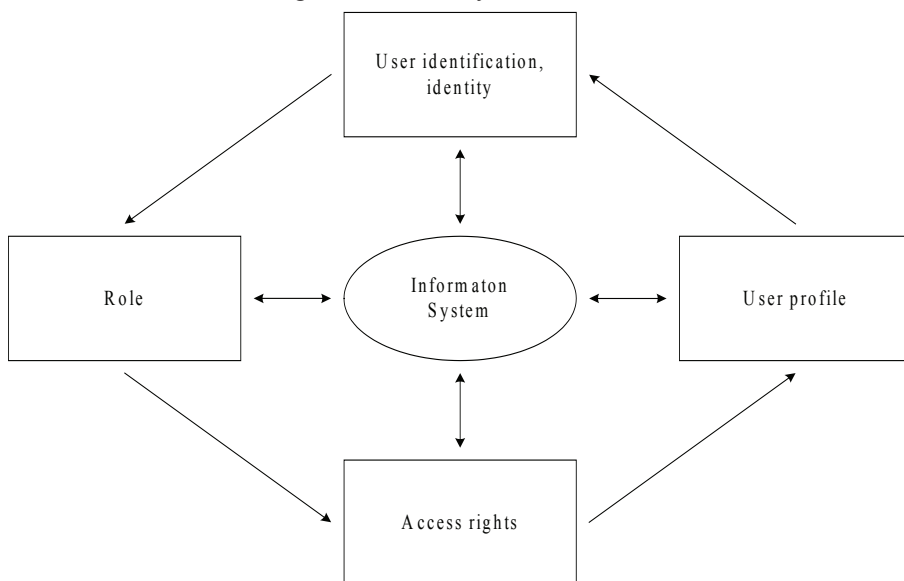
Roles might be connected to business processes (process activities) and organization units. The first enables the functional service of business activity of the company. The later enables the organizational operations and supports decision making. The roles are “invariant”, where only the evolution of information technology or new business processes may affect and change them. Thus the fluctuation of users does not affect the operation of company information systems. Most commercially available, transaction management based IT solutions already use the so-called Role Based Access Control. At the beginning of the role development of the company business process the organization based business role expectations do not match the information management functionality provided by the information systems. One of the most important goals of development of roles is the adjustment of information technology with business requirements (Klarl et al., 2009).

By using *identity* management, we might identify employees and business partners in one or more company information system. In this way we can regulate their access to

different information technology resources. IT links user access rights and denials to the information management functions available in information systems. This becomes very important when the company has several interconnected information technology based information and communication systems. The user access verification (authentication) and allocation of the new access rights (authorization) of new users does not count among its tasks. It tracks the users' individual life cycle (e.g. join the organization, expansion of scope of activity, change of position caused by reorganization, longer unpaid leave or exit).

The organizations operating the information systems by developing, continuous maintenance of *user profiles* and filtering unusual user behaviour may attract the employee attention to involuntary damage too.

Figure 1. User analysis subsections



Source: Prepared by the authors

During user profile development, we may use the log files which contain all data and business transactions started by the users (information request, record new data, data modification or deletion).

By quick analysis of the log data resulting from user behaviour and filtering unusual user behaviour, we may handle information security issues. Unusual behaviour is always a security risk factor (see: „User Activity Analysis” subsection).

#### 4. The grouping of users

It is worth sorting users into user groups before user behaviour analysis. J.M. Stanton et al. (2005) sorts users based on two factors:



- IT and IT security expertise (low or high ...);
- User intention or approach (malicious, neutral and beneficial).

The employee may be dissatisfied (conscious saboteur), naive or hired by a foreign organization and from an analytical point of view the motivation may be important.

This may be completed with habits affecting information security originating from generational differences. According to sociologists the employees may be sorted into five groups regarding their birth date (Lancaster, Stillman, 2005):

- Veterans (born before 1946; they are not relevant as employee);
- „Baby boom” generation (born between 1946 and 1965);
- X generation (born between 1965 and 1980);
- Y generation (born between 1980 and 1995);
- Z generation (born after 1995).

The five generations represent different information security awareness levels where each one has a different information security risk characteristic (Michelberger et al., 2013).

The role in the organization may be a grouping factor too. IT may be worthwhile to distinguish users from middle and senior management as well as professionals responsible for the operation of information systems.

## 5. Security awareness

The users have access to protected information because their scope of activity requires that they have access rights. In case of malicious attacks, it is obvious to the offender to take advantage of security weaknesses.

Analysing user profiles may uncover unusual behaviour and determine negligence and malicious intentions.

Using this information we may inform users about damages implied by their activities, ask them to comply with regulations and improve the working environment.

The implementation, introduction and production of new software assets without adequate security knowledge in the company may affect security awareness as well as weaken information security (e.g. file sharing tool, removable devices, social media sites, etc.).

Users often feel that the information security regulations are ambiguous, hard to comply with, and do not fit together with the company business processes (Albrechtsen, 2007). The roles are not synchronized with the responsibilities. In these cases the users “invent” how to use the information systems. In security surveys and during examinations they declare themselves as conscious users, but their behaviour in case of individual and unusual events shows that they consider more important the practical and quick business results. Situation awareness (Webb, Ahmad, Maynard, Shanks, 2014) greatly influences information security. It would be important for users to understand the importance of the meaning of information for them, what it means now and what it would mean in the future and for what goal achievement it is (will be) needed.

Through event management becomes controllable the so-called “social engineering” audit too. During this activity an independent external expert team tries to



map the weaknesses (security gaps) of the organization regarding information security and test the implemented defence measures. This means testing intrusion (physical too), unauthorized access of information, stealing of assets, installation of spyware, phishing, and sending infected files.

## 6. User analysis

The assessment of user characteristics, habits and behaviour, by analysing the activities and modes of execution of the activities performed with its user profile during execution of its tasks uses the data available in the employee registry of the company, the log entries regarding user activities of the transaction processing systems available in their log files. The information synthesized this way may be used as master data during log file analysis for information security in order to filter unusual user behaviour events and identify information security events. The log analysis may provide new information about users, which can be used to improve the already available user profile.

## 7. User activity analysis

The user activity analysis regarding the amount of information available per user, the resources needed to gather and process it is a huge task in the case of larger organizations, but it is not unimportant in the case of small organizations too.

The manual processing of the security information it is possible in small organizations, but the accessibility for manual processing of the personal and the activity log raw data without automated pre-processing may lead to misuse or abuse.

For the execution of an automated user profile analysis, information about users available for the company should be available in the SIEM system, which processes the user activity information. The information available about users can be categorized into groups of data storable and not storable in information systems. The storage of personal information or information related to persons may violate privacy and other rights relating to personality. During definition, recording and processing of the set of data, privacy and local rights related to personality should be considered in order to comply with legal requirements. Furthermore the security of data - confidentiality, integrity and availability – should be warranted, so only the entitled persons may have access to them, and only when needed.

We may consider master data, the rarely changed personal data and user characteristics description data, needed to build user profiles, which are usually available for the organization in the following databases:

- Registry of employees, which includes:
  - o The employee roles and tasks;
  - o The age group – which generation belongs to;
  - o The position held in the organization;
- Access Control System, which regulates the physical access of the employees, to which buildings and territories has access rights;

- Time and Attendance System, which regulates when the employee has user access to the information systems and from where;
- Directory services which contains:
  - o User identifier of the employee;
  - o The workplace and the contact information;
  - o Group membership, which usually covers and ensures access rights;
- Identity Management System, in case of lack of it, user access control registry, which support the registration, change and removal of access rights for the users;
- Configuration Management Database (CMDB), which records all the assets used, accessed, administered by employees.

To successfully execute user activity analysis further data are needed, which may change continually and are not available in information systems of the organization, but can be synthesized from the entries regarding user activities stored in the log files of the information systems. These may be user behaviour, personality characteristics, helpfulness, typing speed, user aptitude, security awareness, usual login end point, login path and duration, the system commands and their order used in information systems. The small deviations from the user profile perceived during log analysis should be analysed and added to the user profile, while keeping the historical data too. In this way the user profile can be maintained continuously, the bigger deviations might be considered as unusual events and may be subject of further investigation or alert.

From the information security point of view the most important data is the user activity log entries in the log files of information systems. We might consider these monitoring of the user, but their real goal is the identification of unusual events and their use for the improvement of organizational information security. The information systems continually log the activity of the users to allow the identification of user or technical errors and facilitate their remediation and elimination. This information can be analysed and interpreted system by system individually, but in this case conclusions may be deduced for the individual systems only. Because the attacks against information security usually affect more than one information system, their identification is more effective if the analysis is done on all merged log files. The security analysis of user activities plays an important role in the investigation of log file entries originating from security assets and the analysis of network traffic. The analysis is performed in SIEM systems, which gather the log entries from the information systems of the organization, identify activities using complex mathematical algorithms and put together the coherent information of these.

Despite contemporary logging standards, the different information system log events in different formats. Despite formal differences of log entries they contain the most important data in most cases. On the basis of which the following information can be produced:

- Who generated the event;
- What is the subject of the event – what happened;
- When did the event happen;
- Where did the event happen – on which asset;
- Which object happened the event on (file, database, etc.);

- The source of the event – from where was fired the event;
- What was the event aim at.

This makes possible the standardized storage of different kind of event records (SECUROSIS, 2010), which is called normalization and enables the uniform storage (United States Patent, 2014) and processing of the events originating from different system log files. There are information systems which record events repeatedly until the root cause is identified. This makes the filtering of duplicated log entries an important task. In large organizations this means gathering, processing and storage of the huge amount of event records data. The next phase of log entry processing is the correlation of events originating from different information systems. During event correlation the SIEM systems apply complex mathematical models to identify relationships. With the appearance of the APT (Advanced Persistent Threat) attacks event correlation became more and more important, as these types of attacks are prepared and executed during a longer period of time, while, the attacker is waiting for the best moment to execute the intended malicious action and gathers information about the organization, employees and assets.

The realization of user activity analysis is a complex task, implementing it in SIEM systems in most of the cases requires long preparation and usually implies high cost because their operation requires continuous support activities (Shenk, 2012). The SIEM solutions available on the information security market provide different functionality, data processing and reporting speed and they are able to process different amounts of log entries during a given period of time (Butler, 2009). Some of the solutions skip log entries without processing in order to keep the ability of real time analysis. Others aim to do all-inclusive processing and lose the ability of real time reaction to the security events. In most cases the duration of information security attacks is less than one hour, but often it takes only minutes, so the ability to respond to these requires real time alerting mechanisms. In the case of large organisations scalability plays an important role, because their activity generates huge amount of information security data, the processing of which requires significant computing, processing, storage and reporting capacity. Moreover the storage of security data requires well designed data storage structures which support information security, processing of large amount of data and supports the report generation (Shackleford, 2013).

## 8. User activity analysis automation

The size and scope of activities of organizations determine their need of information processing, storage and security. The implemented information processing infrastructure and storage capacities usually fit the needs because the business depends on them. The information security is invisible – in some cases the abuse of it too -, so the implementation of support systems usually does not reach the needed level. For example: there is a log file consolidation solution, but it is only used for security incident analysis.

The processing of available log file entries for user activity analysis can be executed with SIEM systems enhanced with an intelligence layer customized to organizational needs

(Shackleford, 2014). As we have seen, to execute an automated user activity analysis, the setup of several master data files is needed, which are available in information systems depending on the information technology maturity of the organization. The modern SIEM systems are able to import these data automatically. If the master data import cannot be automated, particular attention is needed for refreshing it in time, especially in the case of user account and access rights at creation, change and removal.

The implementation, operation and support of the first generation of SIEM systems was difficult, resource intensive and costly regarding their added value. The minimization of costs and tasks might be achieved by automation of master data administration by importing them regularly through interfaces from other systems or data files and refreshing them using the results of log file analysis. Scientific research is in progress to build a SIEM system which requires minimal configuration and can identify unusual events and information security incidents with high accuracy.

## **9. The role of configuration and change management in user activity analysis**

Configuration management might be considered in the strict ITIL based sense, which covers the maintenance of the configuration items register (information technology assets - hardware, software and network- and users) and their relations in the configuration management database (CMDB), supports answering questions like: "What would be if ...?" based on analysis of asset data available in the database and supports change management; in the broadest sense it covers the configuration item settings maintenance too. The configuration management is in close relationship with IT asset management (ITAM) because it registers the owner, location, responsible maintainers, administrators and users of the IT assets.

Configuration management relies substantially on *change management*, which plays an important role in keeping up to date the configuration item data in the CMDB. The most important role of the change management is to register the IT change requests, track their design and implementation, provides adequate controls to support the successful execution of changes and to register the changes implied in configuration items.

After the approval of the change requests and design of changes it is worth registering the implied changes of IT asset in the IT infrastructure to the configuration database and marking them final, after the successful implementation of the change.

The solutions supporting configuration management may be divided in two groups:

- Solution supporting automated update of configuration items, which monitor continually the information technology infrastructure elements, detects the changes emerging in configuration items and their configuration, in case these are registered among the approved changes in the change management registry, acknowledges them, otherwise alerts the configuration manager about the unapproved change;
- Solutions not supporting automated refresh of configuration items, in this case the update of configuration item parameters, are done manually after implementation if changes.

From the point of view of information security both solutions support the log analysis and the analysis of user activity by providing information to SIEM systems about assets, users, their parameters and relationships by data import through interfaces and historical data query. The configuration management solutions supporting automatic update of configuration item data detect the changes of configuration items and their relations in the information infrastructure of the organization and may analyse these regarding the approved changes in progress and report unapproved changes to the configuration manager while logging the event. The SIEM systems processing the log files, detect the unapproved changes in the IT infrastructure and may report information security events to the administrators.

A well designed and implemented IT operating model and CMDB based IT service management solution may play an important role in user activity analysis, unusual event detection and information security incident identification.

## **10. A possible model for automated user activity analysis**

In the case of SIEM systems transmitting unusual event detection and alert messages to administrator in real time, the minimization of administration is a key factor in order to facilitate operations. This can be achieved by building an appropriate operation model and gathering master data needed to build user profiles automatically from partner systems through interfaces when these data changes happen.

Regarding modern SIEM systems, it is a requirement to provide interface mechanisms to system management and information security solutions (Tarala, 2011), such as directory services, CMDB (Configuration Management Database), incident and change management solutions, IDS (Intrusion Detection System), IPS (Intrusion Prevention System), antivirus systems, proxy servers by querying which may improve the performance of log file analysis and help to improve the detection rate of unusual events and security incidents.

If there are adequately detailed log files available, a new possibility arises for identification of new and changed user role and access right tasks performed by administrators. By querying and using master data available in partner systems the legitimacy of these changes can be verified. If no adequate master data is available the user, role and access right changes might be interpreted as unusual events and administrators should be alerted, who may analyse and acknowledge the changes as new or changed user or may detect an information security event. The maturity of the information technology of the organization and the availability of master data needed for user activity analysis in information systems significantly influences the amount of tasks needed to execute the setup and maintenance of the SIEM system and detection of information security events. During log file analysis new data may be synthesized about users which should be stored historically in the user profile, continually improving them.

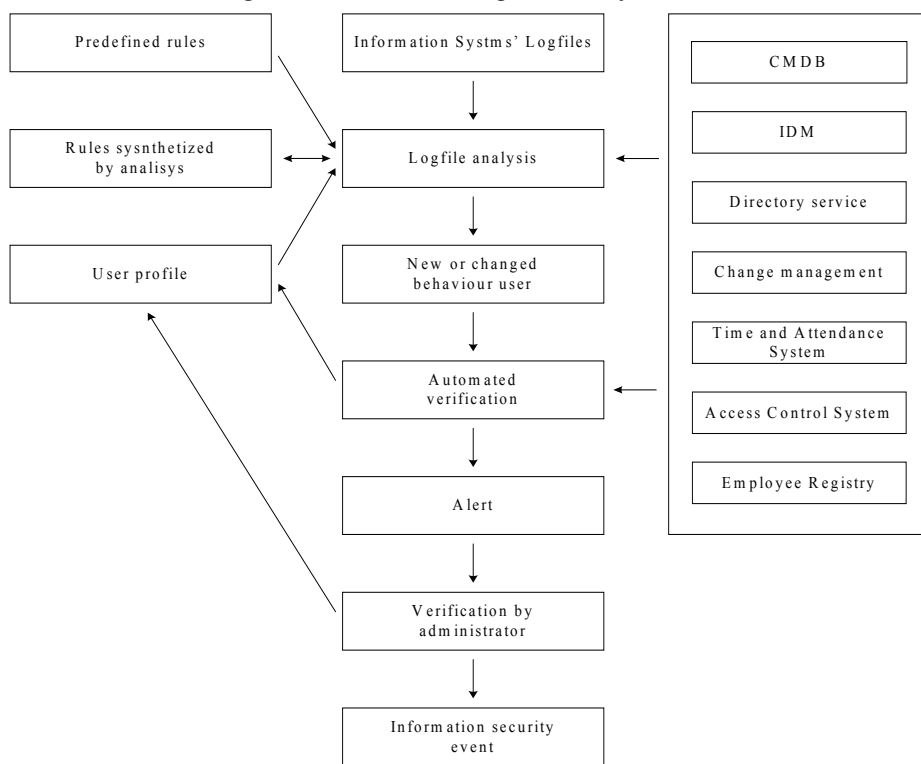
Most organizations do not have all the master data needed for user activity analysis available in information systems, so the all-inclusive analysis of the user profile is not achievable. There are two possibilities available for these organizations to do user profile analysis:

- Skipping the analysis connected to the master data elements missing from information systems, which may lead to loss of unusual event detection and information security events may remain undiscovered;

- Executing the analysis of log entries connected to the missing master data elements, which may produce false alarms.

Both approaches have advantages and disadvantages: if the log analysis is not complete, it can be executed faster, but information security events may remain undiscovered, while the analysis based on incomplete master data records takes longer, are inaccurate and may lead to several false alarms sent to administrators, which means administration overhead for the organization. There exist other configurations available between the two extremes which detect the information security incidents, but the filtering of false alarms does not mean too much administration. The successful SIEM and Log Management Strategies for Audit and Compliance (Swift, 2010) written by David Swift provides useful support for implementation of SIEM systems.

Figure 2. Automated user profile analysis model



Source: Prepared by the authors

## Conclusion

The real scope for the organizations is not the operation of a SIEM system, but:

- Minimization of unnecessary user access rights;
- Special attention and control of system administration activities;

- Identification of unusual events and information security incidents;
- Detection of security holes of information systems;
- Detection and response to attacks originating from inside and outside of the organization against information systems;
- Prevention of information leakage and data integrity assurance;
- Improvement of business continuity;
- Detection of information security awareness gaps and eliminating them;
- Identification of the participants of the events (event management, user identification and configuration management integration).

The implementation, maintenance and operation of SIEM systems is successful, when fulfils the following conditions:

- The number of false alarms and security events is minimal;
- The solution does not impose unnecessary administration burdens to the organization.

## References

- A Frost & Sullivan Market Study in Partnership with ISC2, <http://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf> (27.2.2015.)
- Albrechtsen, E. (2007) A Qualitative study of users' view on information security. *Computers & Security*. Vol. 26, pp. 276-289.
- Butler, J.M. <http://www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755> (5.7.2015.)
- Ernst & Young, [http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/\\$FILE/EY-global-information-security-survey-2014.pdf](http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf) (27.02.2015)
- Karyda, M., Kiountouzis, E., Kokalakis, S. (2005) Information systems security policies: a contextual perspective. *Computers & Security*. Vol. 25, pp. 246-260.
- Kawakami et al. (2014) United States Patent No.: US 8,732,129 B2 Storage System for Managing a Log of Access. United States Patent and Trademark Office
- Kim, D., Solomon, M.G. (2013) *Fundamentals of Information Systems Security*. Jones & Bartlett Publishers, Second Edition
- Klarl, H., Molitorisz, K., Emig, C., Klinger, K., Abeck, S. (2009) Extending Role-based Access Control for Business Usage. *SECURWARE '09, The Third International Conference on Emerging Security Information Systems and Technologies*, pp. 136-141. Athens/Glyfada, Greece.
- Lancaster, L.C., Stillman, D. (2005) *When generations collide*. First Collins Business Edition. New York
- Michelberger, P., Beinschróth, J., Horváth, G. K. (2013) The Employee - An Information Security Risk. *ACTA OECONOMICA UNIVERSITATIS SELYE 2 (1)*. pp. 187-200.



- Miller, D.R., Harris, S., Harper, A., Vandyke, S., Blask, C. (2014) Security Information and Event Management (SIEM) Implementation. McGraw-Hill.
- Park, J., Robles, R.J., Hong, C., Yeo, S., Kim, T. (2008) IT Security Strategies for SME's. *International Journal of Software Engineering and its Applications*, Vol. 2. No. 3, pp. 91-98.
- PwC, <http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#> (27.2.2015.)
- SECUROSIS, [https://securosis.com/assets/library/reports/Securosis\\_Understanding\\_Selecting\\_SIEM\\_LM\\_FINAL.pdf](https://securosis.com/assets/library/reports/Securosis_Understanding_Selecting_SIEM_LM_FINAL.pdf) (7.6.2015.)
- Shackleford, D. <http://www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507> (18.6.2015.)
- Shackleford, D. <http://mpa.co.nz/media/34691/security-intelligence-in-action-sans-review.pdf> (14.07.2015.)
- Shenk, J. <https://www.sans.org/reading-room/whitepapers/analyst/eighth-annual-2012-log-event-management-survey-results-sorting-noise-35230> (01.08.2015)
- Stanton, J.M., Stam K.R., Mastrangelo, P. (2005) Analysis of end user security behaviours. *Computers & Security*. Vol. 24, pp. 124-133.
- Swift, D. <http://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528> (2.7.2015)
- Tarala, J. <https://www.sans.org/reading-room/whitepapers/analyst/implementing-20-critical-controls-security-information-event-management-siem-systems-34965> (1.7.2015.)
- Webb, J., Ahmad, A., Maynard, S.B., Shanks, G. (2014) A situation awareness model for information security risk management. *Computers & Security*. Vol. 44, pp. 1-15.