The deployment of security information and event management in cloud infrastructure

Filip Holik, Josef Horalek, Sona Neradova, Stanislav Zitta, Ondrej Marik
Faculty of electrical engineering and informatics
University of Pardubice
Pardubice, Czech Republic
{filip.holik; stanislav.zitta ondrej.marik}@student.upce.cz; {josef.horalek; sona.neradova}@upce.cz;

***Abstract* - This article deals with the problematics of data safety and security in cloud environment while using Security Information and Event Management (SIEM). This article introduces and critically assesses the basic principles of SIEM in data infrastructure, its deployments in specific cloud environment, and technical requirements for SIEM solution implementation into a cloud environment applied to individual cloud distribution models.**

Keywords—SIEM; cloud infrastructure; AlienVault OSSIM; IBM QRadar SIEM

I. INTRODUCTION

Information system security is still a current topic [1]. News about successful cybernetic attacks appear in both specialized and popular sources [2]. Not only private corporations, but also state institutions and the government are aware of the value of data and information [3]. And it applies twice as much with cloud technology. Methods and abilities of an attacker are more and more sophisticated. It might be difficult to keep an overview of the real state of the infrastructure in large environments and therefore even of possible threats. For this reason it is important to deploy technologies enabling central control of such environment. Such technology is Security Information and Event Management (SIEM) [4]. The main aim of this article is to introduce results of options and approaches of SIEM analysis from the viewpoint of technical requirements and logical links within the boundary of SIEM deployment in a cloud environment. AlienVault OSSIM, the only usable tool under the open-source license at the time of writing this article, and IBM Qradar from the variety of commercial products (in cooperation with the research department of IBM Czech Republic) were selected for the analysis. Collected results were assessed using the SWOT analysis presenting overall results and recommendations for deployment of SIEM in a cloud environment and thus presenting unique knowledge of options of implementing SIEM.

II. SIEM PRINCIPLES

Complex and independent SIEM solution brings specific services and advantages for users according to [2]. Such advantages are:

- *Log management* - each device in the company infrastructure produces a specific type of log files, in which information and events on that device are recorded. This data can be used for obtaining a security picture in case the data is stored in a centralized database and it is mutually correlated.
- *IT standards and legislation* - these are an inseparable part of every security management. If the company wants to present itself as trustworthy, these standards must be kept and thanks to the SIEM solution a particular certificate can be obtained representing a competitive advantage.
- *Events correlation* - this is another key part of the SIEM system ensured by a particular type of artificial intelligence. The amount of information necessary to present in connection with correct assessment of a security risk can in many cases exceed human capabilities.
- *Automatic active response* - these are the consequence of even correlation, in case a security risk is detected, automatic steps preventing security incident can be taken real-time based on available information. Some of these steps can be blocking of a particular port on the firewall or adjusting the access filter. In such case a human would again not be able to react as fast as the SIEM system enables to react. It is necessary to consider that if the configuration is wrong, unnecessary and unwanted steps affecting critical services and applications in the company can be taken.
- *Security of end stations* - this is an important factor within the whole company infrastructure. It is obvious from [5] that the majority of security threats comes from failure of the human factor. End stations are devices that come into direct contact with the employees. These can purposefully or unintentionally cause a security incident. For this reason it is important to monitor the state of an end station, mainly the state of the antivirus program, the state of the antivirus program databases, the state of the firewall and its updates.
- *Centralized security management* - it brings the highest added value. It is common to utilize variety of security tools by various developers, but each product has its own logic, its own administrative console, its own meaning. When the systems do not cooperate, inefficient usage of information provided to the

security teams occurs. Thanks to SIEM it is possible to centrally administer, assess, and report these information. The SIEM solution does not perform any task by itself as it requires information for its operation and it applies that the more information is provided the more useful it becomes. Thanks to centralization the complex solution can be then more than just a mere sum of individual parts.

- *Reporting* - is based on a centralized infrastructure, brings valuable and clear information, based on which the security team can accept critical as well as common decisions associated with managing company security.

A. SIEM Architecture

Based on the above introduced features and services provided by the SIEM solution it is possible to introduce the SIEM architecture itself.

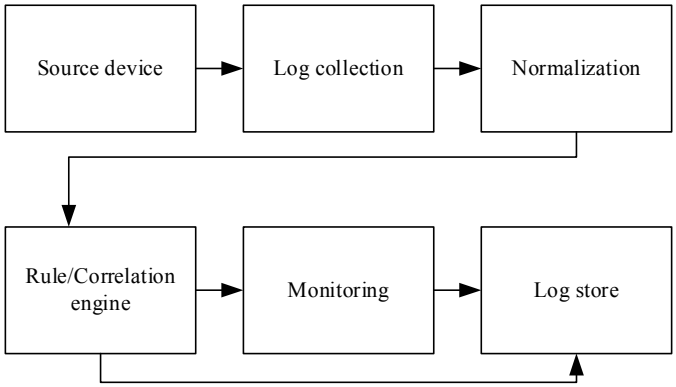

Fig. 1. SIEM Architecture

Just like any other modern technology, SIEM is made up by elementary parts. It is obvious that individual parts more or less vary in individual projects; however, if we speak about SIEM, the solution must contain:

- *A source device* - wide range of devices within the company's infrastructure can serve as a data source. Both devices and applications can serve as a data source. Operating systems, servers, critical applications, network devices, firewalls, antivirus programs, and IDS / IPS systems can be regarded main data sources then.
- *A log collection* - a module ensuring synthesis and analysis of data obtained from individual devices. It utilizes push method which is easier to configure in SIEM and its principle lies in data being sent into the system by the source itself. The SIEM system then serves as a data recipient and does not directly intervene in source managing. An example of this method is the syslog protocol, which is combined with the syslog server. The source is provided a syslog server's IP address and it then receives sent data. Major disadvantage of this method is its security vulnerability as the UDP protocol, which does not ensure the delivery and the integrity of data, is used for communication. Another disadvantage is that by principle SIEM does not have any control over the source. Different approach is the Pull method, more difficult to configure, because SIEM does not serve as a controlling element here and it is forced to request the data from the source. A typical example of it is a database secured by an appropriate password. Here, SIEM must establish a connection to the database via AAA certified methods (authentication, accounting, authorization). The required data is provided using pre-defined methods. The Pull method is thus safer as SIEM knows exactly from which source the data is being obtained. But because SIEM serves as a controlling unit here and request the data, there is no guarantee that the log files are being delivered in real time and the overhead costs are higher. There is then an interval for data requesting set in the system. The duration of such interval is then directly proportionate to data topicality and overhead costs.
- *Normalization* - it is a SIEM system engine for normalizing obtained data for further processing. The method of normalization depends on the specific system and the specific developer/manufacturer. Normalization means converting the original data into a standardized and unified form.
- *A rule/correlation engine* - these are two engines; the rule engine applies rules for reaction to an obtained event. The second, correlation engine, which can be labelled as the SIEM's brain, which, based on event correlation, discovers links posing potential security treats. A series of attacks cannot be discovered based on simple rules, but only thanks to wider context in the system. Thanks to this artificial intelligence it is also possible to restrict occurrences of false reports, which are a frequent phenomenon in the IDS/IPS (Intrusion Detection / Prevention System) without this intelligence. A report, which would normally be ignored or considered unimportant, then can be assessed as an attack after being correlated with information from other security elements. An example can be an unexpected load of database server CPU. It does not have to mean a security incident, but when even other servers show an unusual load of CPU, it might be considered a security incident.
- *Log storage* - it is not only storing data of logged events, but also an overall system storage. Saving such log files and data from these files is the highest priority in SIEM as it is necessary to secure traceability of information and events recorded in SIEM. Security audit can require such data and it is therefore necessary to save them securely and for a reasonable time. Within SIEM, data saving is done in either test or binary form into a database, type of which is again dependent on a specific system.
- *Monitoring* - this part of SIEM stands outside the above introduced sequence. Monitoring in the SIEM concept is interaction with data in the system. The system can process and assess information by itself, but

administrators and SIEM users need to access the overall events. In majority of cases can ensure a particular type of console which can be based on web services or it can be implemented as an individual application.

III. Definition of Technical Requirements for SIEM in Cloud Environment

Technical requirements for SIEM in a cloud environment are one of the most important things to define. Cloud infrastructure is a specific environment distinguished by high scalability, flexibility, being robust, and also abstraction plays its part. Big cloud solutions can contain up to millions of devices, which can seem to the user as one homogenous environment thanks to abstraction. In this connection it is necessary to know answers to the following questions: Which devices need to be observed? How high must SIEM performance be? What storage is needed for the SIEM system? What network environment is required by SIEM? What security rules must SIEM contain?

The first and the absolutely imperative question is determining from which devices data collection may be required. These requirements can vary according to division based on service, therefore the provided list is adjusted accordingly, as seen on fig 2. Because of the heredity logic, the list is ordered from IaaS. The next point, PaaS, as well as SaaS, inherit points presented in IaaS (Infrastructure/Platform/Software as a Service).

DISTRIBUTION MODELS OF CLOUD COMPUTING		
IaaS	PaaS	SaaS
Physical server Hypervisor Virtual machine Operating system Switch Router Firewall IDS/IPS Storage Database VPN	Middleware Platform system Applicaton code	Applicaton Applicaton data

Fig. 2. SIEM data sources in the cloud

The SIEM systems are characterized by two basic parameters, Event Per Second (EPS) and Flow Per Second (FPS). EPS represents variety of events which the SIEM system is capable to process in one second. The amount of events generated by the device then depends on both the level of detail of generated log information and on the capability of the device itself. Within operation, Normal EPS (NE) or Peak EPS (PE) can be determined. Normal EPS is the amount of events generated on a particular device during normal operation. Peak EPS is a value representing the amount of events generated on a source in case of peak operation, i.e. in case of a security incident. It is a sort of an extreme, therefore this value is determining mostly in the case of a security incident when SIEM must be able to process all these events. For a cloud environment it is difficult to determine a particular number, the number of devices of SIEM sources may range from units to millions. The number of networks and subnetworks, which can separate the attack, is also a factor. Also, the area of infrastructure affected by the security incident is another factor.

The FPM unit then logically represents the amount of flow per minute. The principle of establishing the value of FPM is much easier than with the EPS unit, because the majority of devices offers statistics of data flow in the FPS unit. Based on this value it is then possible to establish required FPM value in the needed network segment. FPM values can vary significantly depending on the environment and is thus not relevant to state estimates for the cloud environment. In this case, individual approach is necessary.

With storage it is imperative to have an overview of the volume and the size of data necessary to store. As an example, average file size of 300 bytes can be assumed. In a company where 20 000 EPS are generated during an 8 hour incident, it is equal to 576 000 000 records, which means 172,8 GB of data. If one wants to be really sure, the theoretical value of maximum needed storage in TB for particular time period can be established based on the following equation:

$$\textit{Maximum needed space} = (\textit{total value PE} \times 300 \times \textit{time interval in seconds})/1024^4 \quad (1)$$

The result of the equation above is a value of needed space when the infrastructure is under attack for the whole duration of the time interval. From the network operation point of view it is possible for the SIEM system to deploy current network environment or it is possible to dedicate independent networks. Using the current network means lower implementation costs, but it is necessary to think about the data load of the network thanks to information transfer into the SIEM system. Dedicated network means sufficient financial costs, but the operation will be separated from the network, which serves for cloud services itself. Maximal data flow can be computed by:

$$\textit{Maximum data flow} = (\textit{total value PE} \times 2400)/1024^2 \quad (2)$$

As it can be assumed, the data flow will not be significant from the viewpoint of current network environments and it can be said that there is no need to dedicate an independent network for the SIEM system for performance reasons in majority of cases. Again, the particular environment is a factor and an individual approach is necessary.

The last important aspect is related to the SIEM's capability to identify threats within the cloud environment. In the cloud environment, SIEM must be able to detect network security threats, threats caused by faulty configuration or malicious software, security threats related to the access interface, security threats of cloud abuse, security threats related to accounts and shared tools.

IV. Deployment of the SIEM Solution in the Cloud

Three main types of diversified services, which run within the scope of this technology and which require individual approach in connection with deploying SIEM, exist in cloud computing. The SIEM system is a technology serving to

information security management to reach established objectives. These objectives originate mainly from legislative requirements and from requirements of international standards. The SIEM systems provide a central overview of information and organization information infrastructure events thanks to infrastructure monitoring and log files analysis. Thanks to normalization and correlation, the SIEM systems are capable of distinguishing real security incidents from those less serious or false ones. Often variety of options of generating reports provides the management with regular and detailed overview of incidents and events in the information infrastructure. Based on this it is possible to face future incidents better and to improve the overall security environment of the organization. These reports are also a key factor for reaching set objectives.

A. SIEM and IaaS

Cloud provider of the Infrastructure as a Service offers, for a fee, information performance available upon request mainly in the form of virtual tools. It is mainly sources as shown on fig. 2. Sources such as switch, router, firewall, and other network elements can also contain protocols enabling the analysis of the ISO/OSI model 4th layer, e.g. NetFlow protocol. In case of IaaS it is a critical group of information. From the viewpoint of deploying the SIEM systems in this type of cloud it is an environment, which is the most natural for the SIEM technology and therefore options for deployment are the highest. The reason is that the cloud infrastructure with its elements does not differ from non-cloud environments much. Virtualized information tools are very common and thus terms such as hypervisor and virtual machine are not the privilege of clouds only. This fact of course is good news for the SIEM systems, which are not necessary to significantly adjust for the IaaS infrastructure. All presented sources can be connected by the SIEM technology as all these elements contain a particular method of logging. In case of using redirecting the output of the syslog server, the situation is simple. A problem can occur with the pull method when it is necessary to connect to the server directly and therefore an appropriate plugin must be present. A typical example of deploying the pull method is Microsoft Windows operating system.

From Gartner's [6] study of security threats it is obvious that it is necessary to take into account all presented threats for the IaaS environment. The ability to detect such threats is listed in other subchapters for each individual solution. Generally, the SIEM systems contain rules and definitions for these threats, similarly as with the infrastructure those are threats which do not occur in the cloud environment except for one - cloud service abuse. The biggest challenge for SIEM is scalability of cloud IaaS environment. It is not the scalability of the physical infrastructure, but the flexibility of deployment of virtual machines initiated by the user. This fact affects deployment in two aspects, performance and source connection.

The SIEM systems must be designed with performance reserve, because planning necessary performance may be difficult with regard to dynamic fluctuation of virtual machines in the cloud. From the viewpoint of these sources to SIEM it is again a problem with dynamic fluctuation. Images of operating systems or virtual machines containing a syslog server can be configured automatically using scripts, but this does not apply to situations when the pull method has to be deployed. Furthermore, within the SIEM system it is necessary to register a particular source in some way and this task is performed by the system administrator. A situation, when the administrator manually registers and deletes such sources during a high fluctuations of virtual machines or other virtual devices within IaaS, can occur.

AlienVault OSSIM and IaaS

One of the possible SIEM solutions in IaaS cloud environment is Open source project AlienVault OSSIM. For the possibility to deploy this project in IaaS, it is necessary to define two aspects, the ability to connect sources and performance. In the first of these aspects, OSSIM is a competitive alternative to commercial solutions. The offer of default plugins in OSSIM deployable within IaaS is wide. OSSIM does not operate with the option for the pull method, that is where OSSIM fails and can then be deployed mostly for sources enabling redirecting to a specific IP address, which partially restricts its deployment. Instead of the pull method, OSSIM uses deploying agents functioning on the pull method principle. However, deploying these agents is also restricted. It is mostly designated for operating systems where an open-source tool OSSEC serves as an agent. In case of network traffic monitoring, OSSIM offers a solid overview of events on the networks thanks to a variety of tools. With the performance aspect, the situation is more complicated mostly because of the unscalability of the solution. The OSSIM server alone can process 10 000 EPS. In the model example it was shown that within the cloud infrastructure 10 000 EPS is a restrictive value. Theoretically, it is possible to deploy more OSSIM implementations for particular type of device, but thus losing central control and deploying such decentralized SIEM system is not suitable. The last assessment deals with the ability to detect security cloud threats. Here, OSSIM offers abilities of detection in categories of network attacks, misconfiguration, DoS attacks, malware, and bruteforce attacks. This group only covers a narrow selection of security threats, these definitions would need to be completed to be used in a cloud [7]. OSSIM offers the option of configuring one's own definitions. Deploying open-source OSSIM within IaaS is not impossible, however, there is a number of limiting factors restricting such option.

IBM QRadar SIEM and IaaS

When deploying the commercial product QRadar SIEM by IBM, it is expected that it will show high qualities in the IaaS environment. The positive is that these expectations are met. From the viewpoint of connecting sources, IBM QRadar SIEM system meets demanding criteria. Thanks to fully-fledged deployment of both push and pull methods, rich configuration options, and wide support of logging sources, QRadar offers wide spectrum of connectable sources. Performance is another strength of IBM QRadar SIEM. The system offers almost unlimited options of scalability and performance enhancing thanks to the distributed infrastructure. Overall performance comes from the summary of

performances of individual flow and event processors. In the field of accessible rules for threat detection IBM QRadar SIEM is again on top. There are 25 categories of rules largely covering the presented threats. For the needs of the cloud it would be necessary to add more rules especially for the area of threats of data theft, data loss, and cloud service abuse.

B. SIEM and PaaS

Cloud service of the PaaS type offers a platform for development of cloud and other applications. PaaS cannot be run without elements contained in IaaS; it is highly plausible that PaaS provider will require the same conditions. But unlike the IaaS provider, the PaaS provider will also be interested in middleware integration, a platform system and the code being developed. Just like in the case of IaaS, even here all introduced security cloud threats apply. That is given by the PaaS containing the same elements and principles as IaaS. Had this IaaS layer been separated and threats concerning only the PaaS extension layer would be considered, types of threats, such as data theft, data loss, DoS attacks, and problems connected with shared sources, would disappear. Threats concerning account corruption, unsafe interface, and cloud service abuse would be critical. The SIEM system is constructed in such a way to assess potential threats based on information and events happening in the environment. It is not adjusted to, for example, virus detection based on scanning code principle. In this case the SIEM technology is not able to detect the development of a potential virus or other malicious software.

AlienVault OSSIM and PaaS

AlienVault OSSIM cannot be unambiguously recommended to be deployed in IaaS, and it is even less recommended for PaaS. As it was already mentioned, SIEM systems are not primarily designated for environments by which the PaaS service is distinguished. In more natural environment, which is IaaS, OSSIM shows significant restrictions. Within PaaS these restrictions even escalate. Assuming that OSSIM was deployed only for middleware and the platform system and the components would contain redirecting of logging record outputs generating less than 10 000 EPS, it would be possible to deploy OSSIM for PaaS.

IBM QRadar SIEM and PaaS

IBM QRadar SIEM proved strong potential in possibility of deployment in IaaS cloud service. Just as with general viewpoints of deployment of SIEM in PaaS, even QRadar SIEM has some limitations. Thanks to the before mentioned distributed architecture, there is no problem with the performance side for IBM systems. With integration of middleware or platform system, QRadar has to rely on the logging abilities of the components. To some extent it would be necessary to define essential rules, but QRadar would be able to provide basic information without any major intervention. For monitoring and testing a code being developed within the platform, not even IBM QRadar SIEM offers specific options. Deploying IBM QRadar SIEM within PaaS cloud service is possible with slight adjustments. The biggest limitation is the impossibility to test the code being developed.

C. SIEM and SaaS

Model of a SaaS cloud service offers a finished application communicating via a web interface. The SIEM system in this service model is based on similar assumptions as with the PaaS service model. The relationship of IaaS and PaaS is similar to the relationship of IaaS and SaaS. Even here, elements of IaaS, extended by a particular platform hosting the target application offered to the user, are the basic layer. Unlike PaaS, the service operator does not require the SIEM to possess abilities to monitor code. It would be probably very useful to integrate middleware and platform hosting as a particular application. To deploy SIEM technologies in SaaS service model, the same rules and laws as mentioned above apply. Some differences and uniqueness of the SaaS model lies in the applicability of mentioned threats. Here, the list is reduced by the possibility of cloud service abuse as the complete cloud model and therefore the application itself is administered by the operator. Focus then shifts mostly to threats connected with IaaS environment elements. Mostly it is the activity of the application itself that is observed with SaaS. Then audit records of user access are tracked, which is no problem for the SIEM system. In SaaS model, the SIEM technology faces mostly the disunited format of logging records of various applications. Then the focus is shifted to the ability to analyze the 7th layer of the ISO/OSI model. On the contrary, the problem with dynamic scalability disappears as extensions are under the supervision of the operator.

AlienVault OSSIM and SaaS

The same results as for OSSIM in PaaS model apply here for the SaaS model. OSSIM cannot be recommended for the SaaS model for several reasons. The first reason is the need to integrate elements from IaaS for complete monitoring. Here, OSSIM is already not suitable. Its deployment is possible only as an application access auditor. Analysis of the 7th layer of the ISO/OSI model is not offered by OSSIM, which limits its deployment. Deploying SIEM only as a particular auditor then makes no sense.

IBM QRadar SIEM and SaaS

For IBM QRadar SIEM both the SaaS and the PaaS environments are suitable equally. Even here it is necessary to perform normalization or configuration adjustments of rules. However, overall success of this product is determined by its ability to analyze the 7th layer of the ISO/OSI model. That is possible thanks to QFlow collector hardware probe. Thanks to the variety of integration options, QRadar is equipped for collecting information of process data of an application. Just like in other cases, it is dependent on the logging abilities of the application itself. Thanks to a scalable architecture, necessary performance, which is the sum of EPS and FPM from IaaS, PaaS, and SaaS environments, is secured. Deployment of IBM QRadar SIEM for needs of SaaS is plausible, however it is necessary to take configuration interventions into account.

V. SWOT ANALYSIS

Strengths - performance scalability, IaaS environment, source integration, rules configuration, analysis of the 1st - 4th

layer of the ISO/OSI model, central security management, meeting security requirements, reporting, behavioral assessment, ability to provide central and clear picture of security of the whole infrastructure across various models of cloud services. Reports also serve as auditing tools helping meeting strict security standards and legislature requirements. From the technical viewpoint, the SIEM technology is very well prepared for analyzing the 1st - 4th layer of the ISO/OSI model. Modular architecture ensures well scalable performance of the whole solution.

Weaknesses - open-source, PaaS and SaaS environments, source scalability in IaaS, manual sensor registration, partial coverage of cloud threats, price of commercial solutions. Weak sides of the SIEM technology are based mostly on the specific cloud environment. SIEM was a disappointment in the area of open-source. Here, deployment is almost impossible or possible only with huge limitations. The size of the environment plays a significant role as performance is a limiting factor. The inability to scale a solution in a cloud environment is a significant downfall. Another obstacle is the absence of long-term recording of logging records for audit records. The SIEM system is deployed mainly to reach a certain standard, alternatively to meet legislation requirements. Integration into the IaaS environment belongs among the strong sides of the technology, but that does not apply to PaaS and SaaS environments. Not that it would not be possible to implement SIEM in these environments, but because many more configuration interventions need to be performed in order to achieve respecting requirements. Only sensor scalability is missing for the IaaS to be perfect. SIEM technology is generally more of a static element of the infrastructure. Meaning that after implementation the source fluctuation is not very high. In any case, some security threats, such as problems within shared tools, or security of the API interface, are difficult to uncover for SIEM. In the default state there are no defined rules defining cloud service abuse for, for example, botnet network or for illegal storage. Here, the responsibility is shifted to the implementer.

Opportunities - open-source, cloud environment and integration, legislature. It is mostly the area of open-source, where only one universal system, AlientVault OSSIM, exists. But even that cannot be recommended for deployment in a cloud environment. The performance of the whole solution is a true handicap. Generally, it is a big opportunity for the cloud environment itself. For SIEM it is mostly a question of dynamic scalability and coverage of as large spectrum of threats as possible. From another viewpoint, the integration of the SIEM technology into the cloud as an independent service is an opportunity. That might be an interesting choice for users and a service, which will of course require a different approach. Just like as it is applied with other technologies, which emigrated into the environment of cloud services.

Threats - dynamic cloud environment and diversification of sources requiring the pull method. The biggest threat is possibly cloud dynamism. To some extent it depends on customer expectations, to what extent they will require integration into the environment. Nevertheless, the SIEM systems must change their philosophy in this area. Now, the SIEM system is more designated for unchanging static environments. But that is what cloud is not. Another certain threat may be potential logging formats and technologies that will require costly connector development. That might make the price of an already expensive system, which SIEM is, climb higher.

VI. CONCLUSION

Security Information and Event Management is a complex solution for data and information security. SIEM is becoming essential part of information systems deployed in enterprise networks, data centers and industrial power systems. Proposed article described results of the analysis of SIEM deployment into a cloud infrastructure. Results were summarized in conducted SWOT analysis which shown benefits of SIEM deployment into a cloud infrastructure. SWOT analysis also revealed several possible threats and flaws, which SIEM systems brings and which must be taken into the account in design and implementation of SIEM into a cloud infrastructure.

ACKNOWLEDGMENT

This work and contribution is supported by the project of the student grant competition University of Pardubice, Faculty of Electrical Engineering and Informatics Security smart grid networks and cloud computing No. SGSFEI 2015002.

REFERENCES

[1] P. Stephenson, Security information and event management (SIEM). SC Magazine [online]. vol. 7 2013 [cit. 2014-11-08].8.11.2014]. Available from: http://www.scmagazineuk.com/security-information-and-event-management-siem/article/301446/

[2] R. Buyya, J. Broberg, A.GoscinskI. Cloud computing: principles and paradigms. Hoboken, N.J.: Wiley, xxv, 637 p. Computer communications and networks, 2011 ISBN 04-708-8799-0.

[3] Penhaker, M., Krejcar, O., Kasik, V., Snasel., V., Cloud Computing Environments for Biomedical Data Services. In Intelligent Data Engineering and Automated Learning 2012, IDEAL 2012, August 29-31, 2012 Natal, Brazil. Lecture Notes in Computer Science, LNCS Vol. 7435. pp. 336-343. H. Yin et al. (Eds.), Springer, Heidelberg. ISBN 978-3-642-32638-7, ISSN 0302-9743, DOI 10.1007/978-3-642-32639-4_41.

[4] R. Montesino, S. Fenz, W. Baluja, SIEM-based framework for security controls automation. Information Management [online]. vol. 20, issue 4, s. 248-263, 2012, [cit. 17.11.2013]. DOI: 10.1108/09685221211267639.

[5] T. Olavsrud, Most Data Breaches Caused by Human Error, System Glitches. CXO MEDIA. *CSO Security and Risk* [online], 2013, [cit. 4.3.2014]. Available from: http://www.csoonline.com/article/735078/most-data-breaches-caused- by-human-error-system-glitches

[6] J. Fritsch, Enabling High-Risk Services in the Public Cloud With IaaS Encryption. Gartner [online] 30th May 2014.

[7] M. Curtin, K. J. Schmidt, Ch. Phillips, P. Moulder. *Brute force: cracking the data encryption standard*. New York: Copernicus Books, x, 291 p., c2005 ISBN 03-872-0109-2.