Evaluation of Open Source SIEM for Situation Awareness Platform in the Smart Grid Environment

Rafał Leszczyna
Gdańsk University of Technology
Faculty of Management and Economics
Gdańsk, Poland
Email: rle@zie.pg.gda.pl

Michał R. Wróbel
Gdańsk University of Technology
Faculty of Electronics, Telecommunications and Informatics
Gdańsk, Poland
Email: wrobel@eti.pg.gda.pl

***Abstract*— The smart grid as a large-scale system of systems has an exceptionally large surface exposed to cyber-attacks, including highly evolved and sophisticated threats such as Advanced Persistent Threats (APT) or Botnets. When addressing this situation the usual cyber security technologies are prerequisite, but not sufficient. The smart grid requires developing and deploying an extensive ICT infrastructure that supports significantly increased situational awareness and enables detailed and precise command and control. The paper presents one of the studies related to the development and deployment of the Situation Awareness Platform for the smart grid, namely the evaluation of open source Security Information and Event Management systems. These systems are the key components of the platform.**

Keywords—smart grid; situation awareness; SIEM, evaluation

I. INTRODUCTION

The smart grid is a system of systems [1]–[3] built of many components linked together by communication networks and controlled by information systems. The interconnected and interdependent nature of the smart grid opens a way for completely new types of cyberattacks such as Botnets, zero-days or Advanced Persistent Threats (APT). The cyber threats are becoming highly sophisticated. Also, attackers are no longer amateurs. They are now very skilled and organised professionals capable of launching complex and coordinated attacks using sophisticated tools [1]. Additionally to that Industrial Control Systems (ICS), which are a crucial part of the smart grid, bring in multiple vulnerabilities to the grid ICT infrastructure [4].

To counter the evolved, highly sophisticated threats, new cyber security technologies are required, such as Security Information and Event Management (SIEM) systems, application whitelisting, or Trusted Platform Modules (TPM) [1], [2]. Developing and deploying an ICT platform for wide situational awareness became a key action recognised by large standardisation bodies, such as the National Institute for Standards and Technology (NIST) [5], [6]. As situation awareness for the smart grid is a new research subject there have been only a few studies which address it so far. Alcaraz and Lopez proposed and evaluated a model based on Wireless Sensor Networks (WSNs) and cloud computing, which takes the ISA100.11a standard as a reference for managing different types of ICS incidents [7]. Situational Awareness Reference Architecture (SARA) is an ICS-focused project orientated towards compiling and publishing an applied guide to the processes, practices, standards and technologies which facilitate the establishment of situational awareness [8].

This paper presents one of the studies related to the development and deployment of a situational awareness platform for the smart grid related to the assessment of key components of the situation awareness platform i.e. the SIEM systems. It is worth noting that the results of the evaluations can be also useful in the development of other architectures for detecting and reporting smart grid cyber security incidents.

II. SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEMS IN SITUATION AWARENESS

A. Situation Awareness (SA)

There are many definitions of Situation Awareness (SA) [9], [10] from which Tadda and Salerno adapt the one of Endsley [11] to the area of Cyber Situation Awareness: "*Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority.*" [10]

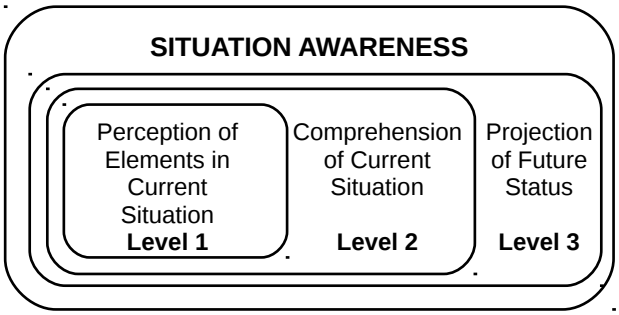

Fig. 1. Levels of situation awareness in the model Endsley [11]

This is a preprint of the paper presented on the
11th IEEE World Conference on Factory Communication Systems
WFCS'15, 27-29 May 2015, Mallorca, Spain.

Cite as: **Leszczyna R., & Wrobel, M.R. (2015). "Evaluation of Open Source SIEM for Situation Awareness Platform in the Smart Grid Environment". Proceedings of the 11th IEEE World conference on Factory Communication Systems, Palma de Mallorca, Spain**

Endsley provides a reference model for situation awareness, which includes three levels (see Fig. 1.).

Perception is the lowest level of situational awareness. It provides information about the status and behaviour of relevant elements within the environment and represents it in a conceived form. Without a correct perception of important environmental elements, the probability of forming a distorted view of a situation increases dramatically [10]. *Comprehension* of a situation is related to combining, interpreting, storing, and retaining information. It extends perception with the integration of multiple pieces of information and the determination of their relevance to established earlier objectives, which can result in inferring or deriving conclusions about the objectives. Comprehension provides a structured outlook of the current situation by determining the significance of objects and events [10]. *Projection* is the top level of situation awareness. It is defined as the ability to make predictions based on the outcome of comprehension (and perception) [10]. McGuinness and Foy [12] extended the model by adding a fourth level, called *Resolution*, which aims at identifying an optimal path to achieve the desired state change to the current situation. Resolution is based on choosing a single course of action from a subset of available actions [12].

Situation Awareness is not limited to cyber security. In the smart grid environment studies are also conducted on energy-aware information systems, which collect and analyse energy data to optimise energy consumption [13].

B. *Security Information and Event Management Systems*

Developing situation awareness platforms for the smart grid is a new trend in smart grid research and only a few pilot architectures have been proposed so far [14], [15]. In the existing implementations, the process of comprehension is supported by Security Information and Event Management (SIEM) [14] systems, which are specialised tools responsible for processing the large amounts of data available in the grid [16]. The main task of SIEM systems is to aggregate and normalise data from different sources, provide constant access to information about events, correlate events and issue alert notifications when a threat is detected [17], [18]. Based on the consolidated outcome of a SIEM system, a human operator can make decisions in response to the alerts issued [18].

During the analysis, three open source Security Information and Event Management systems have been identified, which are being actively developed [19]–[22]: AlienVault OSSIM [19], Cyberoam iView [20] and CS Prelude [21]. They are open source and distributed under GNU General Public License (GPL), which means that they can be used and modified free of charge. However, none of them is developed in a fully open model because they are offered by commercial companies instead of open communities. Due to the vendors' business models, the available open source versions of their systems have limited functionality, require commercial sensors or are dual-licensed.

III. EVALUATION CRITERIA

Two approaches to the evaluation of selected SIEM systems were considered. The multi-step methodology for software statistical evaluation proposed by Anderson and Chen provides a step-by-step approach for the consideration of subsequent issues, such as performance evaluation or the quality of the model [23]. The other approach, proposed by Sahay and Gupta, defines a software selection model and introduces the software Solution Merit Index (SMI) as the sum of percentage scores of attributes that are classified hierarchically [24]. For reasons of greater flexibility and adaptation, SIEM systems evaluation was based on the Sahay and Gupta software selection model.

According to this model, all software selection factors are divided into two groups: primary and secondary drivers. The first group contains essential requirements and facilities, whereas all non-essential attributes are included in the secondary drivers group. [24] Due to the specific nature of the open-source software the assignment of primary and secondary drivers required some modifications. As a result, the first group of drivers contains only the attributes associated to the entire life cycle of a SIEM while the second group includes the drivers which are significant at the deployment stage. The primary drivers group contains "Features" from Sahay and Gupta approach, which are the most important system requirements, essential from the users' point of view.

The drivers related to "Technology" and "Support", such as hardware requirements or portability were moved to the second group as they have secondary importance concerning the operational stage of a system. These drivers have the greatest effect at the initial stage of the system deployment, but during system operation they are less important. For instance, when deploying an open-source system, insufficient technical support is often a problem. Therefore resources must be assigned to the system installation and configuration. However, when the system is installed and configured, the number of resources can be (often significantly) reduced.

Primary evaluation criteria were identified based on the analysis of desirable features of SIEM systems [25], [26] as well as the criteria for the evaluation of intrusion detection systems. Secondary criteria were derived from well-known software engineering non-functional requirements. Fig. 2. shows the hierarchical structure of evaluation criteria.

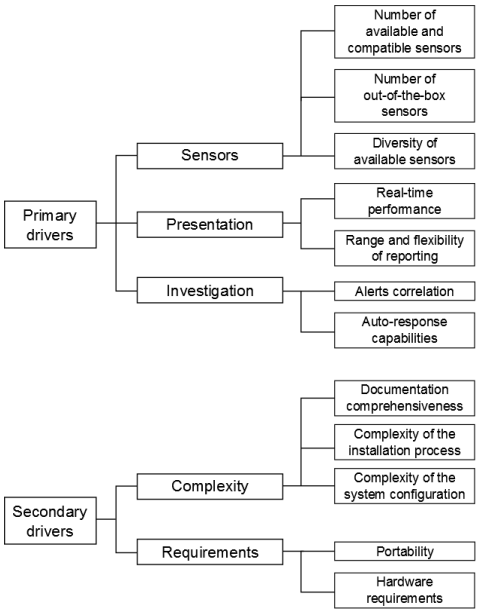

Fig. 2. Hierarchical structure of SIEM systems evaluation criteria

IV. EVALUATION OF OPEN SOURCE SIEMS

According to Sahay and Gupta model [24], Solution Merit Index for each of the SIEM systems evaluated can be calculated using the following formula:

$$SMI = w_p f_p + w_s f_s \quad (1)$$

The symbols f_p and f_s denote percentage based scores due to the primary and secondary criteria groups, respectively, and w_p and w_s are their weights. Considering the importance of groups, weight for the primary group was set to 0.6, which edor the secondary to 0.4. The percentage based scores for criteria groups can be calculated using the following formula:

$$f = \sum_i \sum_j w_i w_{ij} \frac{S_{ij} \cdot 100}{SS_{ij}} \quad (2)$$

Where w_i stands for weight assigned to the ith criteria subgroup, w_{ij} - weight assigned to the jth criterion of the ith criteria subgroup, S_{ij} - total score earned by the jth criterion of the ith subgroup and S_{ij} - maximum score which could by earned by the jth criterion of the ith subgroup. The weights, presented in Table II, were chosen arbitrarily based on the importance of the desirable features of a SIEM in the context of smart grids and ICS.

Each criterion was rated on a scale from 0 to 5 depending on how far they were satisfied for each SIEM evaluated. The actual values were chosen as relative values. It means that in each assessment the rating of 5 was always assigned to the SIEM which satisfied a particular criterion most completely. The remaining SIEMs were given proportionally lower (or the same) scores based on the difference between them and 'the best' SIEM. The value of 0 is assigned in the case when a criterion is not addressed at all.

TABLE I. SENSORS SUBGROUP EVALUATION

Number of available and compatible sensors		
OSSIM	9 native, compatible with over 2000 external	5
Prelude	9 native, compatible with 42 external, open architecture to add 3rd party agents	4
iView	13 (only 4 open source), no bundled sensors, all have to be installed and configured manually	2
Number of out-of-the-box sensors		
OSSIM	Munin, fprobe, Nagios, Nfdump, ntop, OSSEC, Suricata, Nessus, Squid	5
Prelude	AuditD, Nepenthes, ufwi-filterd, OSSEC, Pam, Samhain, Sancp, Snort, Suricata	5
iView	None	0
Diversity of available sensors		
OSSIM	Network resource monitoring, network traffic collector, IDS, vulnerability scanner	4
Prelude	Access monitoring, honeypot. authenticating firewall, integrity checker, IDS, network traffic collector and monitor	5
iView	None	0

For instance, see the 'Number of available and compatible sensors', in Table I. This criterion is most completely satisfied by OSSIM, which includes 9 native sensors and is compatible with as many as two thousand external sensors. Thus OSSIM received the value of 5. Prelude includes 9 native sensors, the same as OSSIM, and is open to 3rd party agents, but is compatible with 'only' 42 external sensors. This means that the level of fulfilment of the criterion is slightly lower than in case of OSSIM. Thus Prelude was assigned a score of 4. iView received the score of 2, because it does not have bundled sensors and is compatible with only 13 sensors, all of which need to be installed and configured manually. This means that the criterion fulfilment is visibly lower than of Prelude. For all of the criteria such analysis and evaluation was carried out. Table II presents a comprehensive summary of the evaluation scores for each criterion.

TABLE II. DETAILED EVALUATION SCORES

Criteria	OSSIM	Prelude	iView
Sensors (weight 0.5)			
Number of available/compatible sensors (weight 0.4)	5	4	2
Number of out-of-the-box sensors (weight 0.3)	5	5	0
Diversity of available sensors (weight 0.3)	4	5	0
Presentation (weight 0.2)			
Real-time performance (weight 0.4)	5	3	3
Range and flexibility of reporting (weight 0.6)	5	2	3
Investigation (weight 0.3)			
Alerts correlation (weight 0.7)	5	5	1
Auto-response capabilities (weight 0.3)	5	0	0
Complexity (weight 0.7)			
Documentation comprehensiveness (weight 0.5)	3	5	2
Complexity of the installation process (weight 0.2)	3	5	3
Complexity of the system configuration (weight 0.3)	4	5	1
Requirements (weight 0.3)			
Hardware requirements (weight 0.4)	1	4	5
Portability (weight 0.6)	3	2	5

In the primary group the lowest score in sensors related subgroup has the iView as it supports a significantly smaller number of sensors and none of them are bundled. The top-rated system in presentation criteria is OSSIM, which has the most modern interface and updates information in real time. The investigation criteria are completely fulfilled only by OSSIM. In the secondary group Prelude was top-rated in complexity criteria, as it has the best online documentation, easiest installation process and configuration. The evaluation of hardware requirements was based on information obtained from software vendors and reported by users. Among systems iView has the lowest requirements and therefore the highest score.

V. EVALUATION RESULTS

The primary and secondary percentage-based scores, with the Solution Merit Index of SIEM systems for use in Smart Grid Situation Awareness Platforms are shown in Table III. The results of the evaluation of the primary features of SIEM systems show that OSSIM unquestionably best meets the criteria defined. It scores 97%, with Prelude receiving 76.6%, and iView only 24.2%. With respect to the criteria from the secondary group, the top-rated one was Prelude, with 86.8%. OSSIM and iView were evaluated similarly, receiving 59.4% and 56.6%, respectively. Finally, considering the primary and secondary group weights, the Solution Merit Index for OSSIM is 81.96%, for Prelude 80.68% and iView 37.16%.

The evaluation shows that OSSIM and Prelude systems best meet the selected criteria. This is coherent with authors' subjective feelings after the installation, configuration and testing of each system in a test environment. OSSIM is a complete SIEM system, ready to be implemented in a Situation Awareness Platform. On the other hand, the advantage of Prelude is its modular construction, which enables using various components, such as machine correlation or log analyser, in building a customised SA platform.

TABLE III. EVALUATION RESULTS

SIEM	Percentage-based score		SMI
	Primary	*Secondary*	
OSSIM	97.0 %	59.4 %	81.96 %
Prelude	76.6 %	86.8 %	80.68 %
iView	24.2 %	56.6 %	37.16 %

ACKNOWLEDGMENT

The study presented in this paper is based on work carried out in the DEnSeK (Distributed Energy Security Knowledge) project founded by the European Commission, Directorate-General for Home Affairs (Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" – CIPS, Project Reference: HOME/2012/CIPS/AG/ 4000003772) and partially supported from the project funds. The authors acknowledge the contributions of the DEnSeK consortium partners involving the development of the business model and their feedback on the data model developed by the authors.

REFERENCES

[1] Y. Aillerie, S. Kayal, J. Mennella, R. Samani, S. Sauty, and L. Schmitt, "Smart Grid Cyber Security," 2013.

[2] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems," *Ind. Informatics, IEEE Trans.*, vol. 7, no. 2, pp. 179–186, 2011.

[3] ENISA, "Smart Grid Security: Recommendations for Europe and Member States," 2012.

[4] M. Cheminod, L. Durante, and A. Valenzano, "Review of Security Issues in Industrial Networks," *Ind. Informatics, IEEE Trans.*, vol. 9, no. 1, pp. 277–293, 2013.

[5] H. Khurana, M. Hadley, and D. A. Frincke, "Smart-grid security issues," *IEEE Secur. Priv. Mag.*, vol. 8, no. 1, pp. 81–85, Jan. 2010.

[6] NIST, "NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards," NIST, 2012.

[7] C. Alcaraz and J. Lopez, "WASAM: A dynamic wide-area situational awareness model for critical domains in Smart Grids," *Futur. Gener. Comput. Syst.*, vol. 30, pp. 146–154, 2014.

[8] ICS ISAC, "Situational Awareness Reference Architecture (SARA)." [Online]. Available: http://ics-isac.org/sara/. [Accessed: 26-Jan-2014].

[9] M. Vidulich, C. Dominguez, E. Vogel, and G. McMillan, "Situation Awareness: Papers and Annotated Bibliography," Jun. 1994.

[10] G. P. Tadda and J. S. Salerno, "Overview of Cyber Situational Awareness," in *Cyber Situational Awareness*, vol. 46, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston, MA: Springer US, 2010, pp. 15–35.

[11] M. R. Endsley, "Toward a theory of situation awarenss in dynamic systems," *Hum. Factors*, vol. 37, pp. 32–64, 1995.

[12] B. McGuinness and L. Foy, "A Subjective Measure of SA The Crew Awareness Rating Scale - GetInfo," in *Proceedings of the first human performance, situation awareness, and automation conference*, 2000.

[13] E. Zampou, S. Plitsos, A. Karagiannaki, and I. Mourtos, "Towards a framework for energy-aware information systems in manufacturing," *Comput. Ind.*, vol. 65, no. 3, pp. 419–433, Apr. 2014.

[14] K. Brancik and G. Ghinita, "The Optimization of Situational Awareness for Insider Threat Detection," in *Proceedings of the first ACM conference on Data and application security and privacy - CODASPY '11*, 2011, p. 231.

[15] F. Baader, A. Bauer, P. Baumgartner, A. Cregan, A. Gabaldon, K. Ji, K. Lee, D. Rajaratnam, and R. Schwitter, "A Novel Architecture for Situation Awareness Systems," in *Automated Reasoning with Analytic Tableaux and Related Methods*, Springer, 2009, pp. 77–92.

[16] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, *Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*. National Institute of Standards and Technology, 2011.

[17] G. Suarez-Tangil, E. Palomar, A. Ribagorda, and I. Sanz, "Providing SIEM systems with self-adaptation," *Inf. Fusion*, May 2013.

[18] I. Aguirre and S. Alonso, "Improving the Automation of Security Information Management: A Collaborative Approach," *IEEE Secur. Priv. Mag.*, vol. 10, no. 1, pp. 55–59, Jan. 2012.

[19] "OSSIM: Open Source SIEM." [Online]. Available: http://www.alienvault.com/open-threat-exchange/projects.

[20] "Cyberoam iView : The Intelligent Logging & Reporting Solution." .

[21] "Prelude-IDS: Prelude Universal Open-Source SIEM project." .

[22] R. H. Syed, M. Syrame, and J. Bourgeois, "Protecting Grids from Cross-Domain Attacks Using Security Alert Sharing Mechanisms," *Futur. Gener. Comput. Syst.*, vol. 29, no. 2, pp. 536–547, Feb. 2013.

[23] E. Anderson and Y. Chen, "Microcomputer software evaluation: An econometric model," *Decis. Support Syst.*, vol. 19, no. 2, pp. 75–92, Feb. 1997.

[24] B. S. Sahay and a. K. Gupta, "Development of software selection criteria for supply chain solutions," *Ind. Manag. Data Syst.*, vol. 103, no. 2, pp. 97–110, 2003.

[25] J. Schütte, R. Rieke, and T. Winkelvos, "Model-based security event management," in *Computer Network Security*, 2012, pp. 181–190.

[26] J. Butler, "Benchmarking security information event management (SIEM)," A SANS Whitepaper, 2007.