Behavioral Analysis of SIEM Solutions for Energy Technology Systems

Tomas Svoboda(✉), Josef Horalek, and Vladimir Sobeslav

Faculty of Management and Informatics, University of Hradec Kralove, Hradec Kralove, Czech Republic
{tomas.svoboda,josef.horalek,Vladimir.sobesdlav}@uhk.cz

Abstract. The aim of this article is to analyze SIEM solutions. Emphasizing the use of these systems to ensure data confidentiality, availability, and integrity monitoring energy technology systems. First, the issue of security in the area of energy systems is introduced. In order to maintain the availability, confidentiality and data integrity, the user behavioral analysis modules in SIEM systems are also introduced. The next section presents specific SIEM solutions that can be currently used not only in ICS environments and which will be subject to comparative analysis. This is IBM Security QRadar SIEM and LogRhythm NextGen SIEM. What follows is the introduction and implementation of modules for user behavioral analysis in the mentioned SIEM solutions, including testing own Use Case for testing user behavioral analysis modules. The results of the comparative analysis of user behavioral analysis modules in selected SIEM solutions are presented in the last section.

Keywords: SIEM · Qradar · LogRhythm NextGen SIEM · User and entity behavioral analysis · IBM sense · CloudAI

1 The Issue of Technological Power Systems Safety

Energy technology systems are systems that are used for power system management, or voice communication system; they are also used in management process of power system [1]. These systems are critical in terms of securing power supplies from the producer to the final consumer and have a major economic impact on the functioning of modern society as a whole. In order to ensure reliable electricity supply, the confidentiality, availability and integrity of the data that is crucial to ensuring the correct operation of the power system must be ensured for these systems [1, 2]. Energy technology systems have been vulnerable for decades. Nowadays, the seriousness of potential threats and related cyber-attacks that energy networks and systems can affect become fully understood [3]. The components currently used in energy systems and primarily supporting IT systems are largely dependent on the use of standard PCs and IT technologies. SCADA data servers, SCADA control servers, HMIs, and operator stations utilize standardized operating systems, increasing the risk of potentially exploiting the vulnerabilities of

P. C. Vinh and A. Rakib (Eds.): ICCASA 2020/ICTCC 2020, LNICST 343, pp. 265–276, 2021.
https://doi.org/10.1007/978-3-030-67101-3_21

these systems by intruders and penetrating the power management system [4]. Many of the systems that are currently operating in power systems are out of date. The reason for the obsolescence is the long-term renewal of energy systems, which typically ranges in the decades and the associated cost of this renewal. For the abovementioned reasons, when energy systems are often unable to meet the latest safety recommendations, the likelihood of cyberattacks launched against these kinds of systems is higher [3, 5].

Energy technology systems are systems that are used for power system management, or voice communication system; they are also used in management process of power system. These systems are critical in terms of securing power supplies from the producer to the final consumer and have a major economic impact on the functioning of modern society as a whole. In order to ensure reliable electricity supply, the confidentiality, availability and integrity of the data that is crucial to ensuring the correct operation of the power system must be ensured for these systems [3, 5, 6]. Energy technology systems have been vulnerable for decades. Nowadays, the seriousness of potential threats and related cyber-attacks that energy networks and systems can affect become fully understood. The components currently used in energy systems and primarily supporting IT systems are largely dependent on the use of standard PCs and IT technologies. SCADA data servers, SCADA control servers, HMIs, and operator stations utilize standardized operating systems, increasing the risk of potentially exploiting the vulnerabilities of these systems by intruders and penetrating the power management system [7]. Many of the systems that are currently operating in power systems are out of date. The reason for the obsolescence is the long-term renewal of energy systems, which typically ranges in the decades and the associated cost of this renewal. For the abovementioned reasons, when energy systems are often unable to meet the latest safety recommendations, the likelihood of cyberattacks launched against these kinds of systems is higher (Fig. 1).

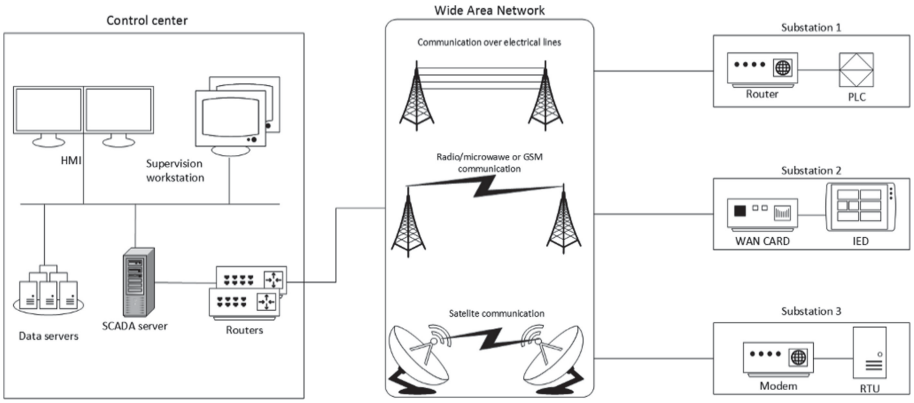

Fig. 1. General energy system architecture. Source: authors

Another potential threat exploitable for technology and energy systems attack, associated with disruption in the availability, confidentiality and data integrity controlling the power system, is at the electric substation level. In particular, the possibility of physical damage to the device type of IED, PLC, RTU, HMI, data ACTIVE servers,

communication facilities and supporting infrastructure, including air conditioning units, power equipment, etc. [8] To avoid or mitigate the attack targeting the physical damage to the equipment should be thoroughly monitor and control the access of all people to the technology rooms where they are located. In order to increase the security and unambiguously identify the persons entering the electric station and at the same time protect the external perimeter, a camera surveillance system is typically installed in the electrical substations. In the case of a suspected breach of the physical security of the technological room, it is appropriate to correlate the record from the access card system and the camera system for unambiguous identification of the attacker [7, 8].

As mentioned above, in the event of a misuse of the threats in energy systems, it is necessary to use tools that are capable of monitoring, logging and auditing industrial control systems, communications and security features, IT support systems and access control systems so that, in the event of disruption, they provide as much available information as possible to detect the attacker, or concerning the causes and techniques that led to security breaches. The great variety and the amount of equipment that needs to be monitored in energy systems poses a problem where a vast amount of information from these devices is generated that needs to be recorded. Together with the expansion and modernization of energy systems, it is growing significantly. [9].

The solution ensuring availability, confidentiality and integrity within the energy technology systems is full implementation of the safety requirements of the international standard ISO 27001. Standard ISO 27001, which is also adopted in the framework of the Czech Republic's national legislation under the Cyber Security Act; the Cyber Security Decree, which defines organizational and technical measures for critical information infrastructure elements, including energy systems.

2 User Behavioral Analysis Utilization to Ensure Energy Technology Systems Safety

User Behavioral Analysis (UBA) is a term that includes tracking, collecting and categorizing user data and activities in their communication in the digital environment, respectively in a computer network environment [10]. Historically, the principles of user behavioral analysis have been developed primarily for use in marketing to predict customer buying behavior. At present, the principles of user behavioral analysis are increasingly used in the field of cyber security, because one of the significant risks of cyber security disruption is the attack vector from the internal environment of the organization, i.e. employees or suppliers of the system. UBA is based on threat detection for employees or system vendors. These are threats related to the misuse of users' identities, deliberate, respectively unintentional user errors that can lead to disruption of data availability, confidentiality and integrity [10, 11].

UBA looks for behavior patterns that are then applied to statistical analysis and algorithms to detect anomalies in relation to standard behavior. For this reason, the principles of behavioral analysis are effective because they focus primarily on user interaction and behavior, not on detecting a suspicious event in the vast amount of information that is collected in the SIEM solution [12].

Based on the above principles, Gartner Inc has created a category called user and entity behavior analytics (UEBA). UEBA focuses primarily on preventing data theft or misusing a computer network when user authentication is broken, and a malware or hacker is operating on its network name.

For the purpose of uncovering these cases, UEBA uses three main components [13]:

Data Analytics - UEBA application identifies user behavior and creates a basic user behavior profile with learned parameters. For further analysis, it uses statistical models and rules to compare user behavior with an existing profile. Data analytics implements data confidentiality.

Data Integration - Flexible UEBA applications are able to integrate both structural and non-structural information into an existing security monitoring system. The information also includes SIEM system logs, data flow data and captured data packets. By implementing the data integration, the requirement for the integrity of the transmitted and stored data is ensured.

Data Presentation and Visualization - The UEBA application, or module, presents the results in an efficient way so that it is easy to read and identify behavior patterns that are associated with unauthorized activity and do not conform to a profile that includes standard user behavior. Based on the violation of the user's standard behavior, their risk score is subsequently adjusted. This is an indicator which corresponds to whether or not the user violates the rules. The higher the risk score, the more rules are violated by the user.

UEBA uses machine learning principles to identify future user behavior. In this case Machine learning means that the UEBA module learns to predict future user behavior based on a defined profile.

3 UEBA Implementation in Selected SIEM Solutions

In order to analyze the possibilities of implementation of UBA, a survey of SIEM solutions with respect to Gartner Magic Quadrant 2018 in the field of SIEM solutions. The selection parameter was also the implementation of UBA functionalities within SIEM. Two solutions were selected for this analysis that meet the above-mentioned requirements. These are IBM Security QRadar SIEM and LogRhythm NextGen SIEM. These solutions and implementation UBA functionalities are presented in detail below.

3.1 AlienVault OSSIM

There are currently no manuals concerning UBA implementation in AlienVault OSSIM. There is only a general UBA discussion. As a part of research, a member of the Business Development, AlienVault OSSIM was approached, who confirmed the existence of the UBA module in AlienVault. After installing AlienVault, it was found that AlienVault does not allow UBA principles to be used, but only contains a basic network behavioral analysis (NBA) module. Therefore, it is an inappropriate solution for comparative analysis.

3.2 IBM Security QRadar

UBA module is not a part of the default IBM Security QRadar installation. After performing the basic QRadar installation, the UBA module was installed within the available Extension Management. To install the UBA module, it is necessary to have the IBM Sense log source used to collect UBA information.

The user data collection is shown in the following figure. QRadar is capable of monitoring user behavior based on incoming events from log sources. From these logs, specific events and data are searched using defined rules to serve as input data for the IBM Sense module, which directly matches UBA applications. Based on built-in or created use case and internal UBA algorithm, it further defines a score that is an indicator of potential user risk.

A prerequisite for using IBM Sense and UBA is the existence of a user name, domain, or other identifying attribute in the messages that QRadar collects (logs or events).

The UBA module extracts the "username" and "senseValue" attributes (that is, defining the increment for the score) from the IBM Sense source events, by which it adjusts, in collaboration with Machine Learning, a specific risk score value for that user. The value of the senseValue is defined differently for each of the set rules from the UBA ruleset and corresponds to the “severity” of the event, respectively to a deviation from standard user behavior. The deviation from the standard behavior can be, for example, identification of the device from which the user has logged in, detection of different IP address of the device, incorrectly entered login data, etc. The more a user violates the set rules, the higher his risk score. In the event that a user exceeds a defined score limit, the UBA module creates an event that responds to the creation of an offense representing an alert for suspicious behavior. In addition, the user is also included in a group of very suspicious users.

3.3 LogRhythm NextGen SIEM

Implementation of user behavioral analysis within the product LogRhythm NextGen SIEM (LogRhythm) coincides only partially with implementations in the solution of IBM Security QRadar. UEBA within LogRhythm consists of two modules:

- Scenario Based Analytics (The UEBA AIE Module).
  - Detect known threats with deterministic threat models (i.e., scenario-based analytics).
  - Baseline behavior across weeks.
  - Detect threats in real time with stream-based analytics.
- CloudAI (ML based statistical analytics).
  - Detect hidden threats with AI / ML.
  - Baseline behavior across weeks to months.
  - Achieve near-real-time threat recognition.
  - Provide high-fidelity data to AI Engine.

Same as in the case of IBM Security QRadar, the UEBA modules are not a part of the default LogRhythm installation. Installation of the UEBA AIE module is done through LogRhythm Knowledgebase. Part of the installation is a set of correlation rules for AI Engine, a set of predefined sheets, which include e.g. the lists of privileged accounts, monitored users, banned countries, etc. Picture 2 shows the UEBA AIE correlation rule package in knowledge-based LogRhythm (Fig. 2).

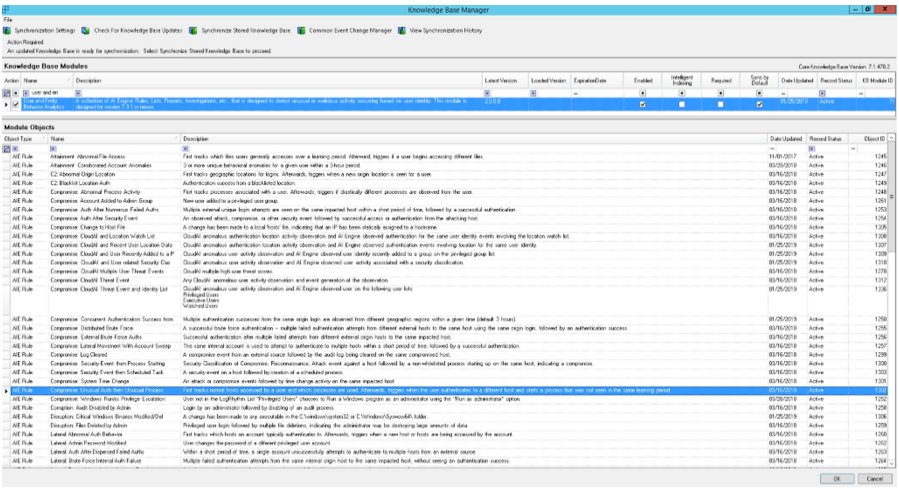

Fig. 2. LogRhythm UEBA AIE module. Source: authors

CloudAI module is not a part of the LogRhythm base license and is subject to separate licensing. Licensing is based on the number of users to which UEBA's rules and principles are applied within the annual subscription. Implementation of UEBA in the LogRhythm solution, compared to QRadar, where the UEBA is part of the basic installation, is financially more demanding.

For LogRhythm solutions AIE and CloudAI there is no need to define any additional log source like in the IBM Sense case at QRadar.

As well as the QRadar, LogRhythm is capable of monitoring user behavior based on incoming events from the source logs. These logs search for specific events and data using defined rules, which are further analyzed by the AI Engine Correlation Rules and CloudAI. To define standard user behavior, thresholds are defined on incoming events. If the threshold is exceeded, the user's risk score is increased.

In particular, the Cloud AI module analyses the following parameters: logon/logoff times, locations, system in use, application used and accesses, time slots that match users' working hours at working days.

The deviation from standard behavior can be the same as in the case of QRadar, e.g. identification of the device from which the user has logged in, detection of different IP address of the device, incorrect login data, etc. The more the user violates the set rules, the higher his risk score.

4 UEBA Modules

This section also demonstrates the usage of its own use case in two of UEBA modules.

4.1 Incorrect Authentication

The first case of use concerns the possibility of UEBA detection of incorrect input of authentication data. The process of incorrectly entering authentication data may not indicate the possibility of attacking the infrastructure if the user mistakenly enters the password. In the case of frequent occurrence of incorrect input of user authentication data, this activity is the reason for this suspected unauthorized access to infrastructure.

QRadar

In the first step, a rule was created to ensure detection**.** After running the wizard to create an event rule, a rule is generated. The rule is applied when an event specified as QID 28250080 (Failed Login Attempt) is detected. The rule sets attribute values for an event for credibility, relevance, and severity. In addition, a new event will be created. This event modifies the UEBA module score for the user who made the bad login. In addition, a text explaining the use case is displayed. The event falls within the IBM Sense log source and is evaluated by other attribute values for severity, credibility, and relevance (Fig. 3).

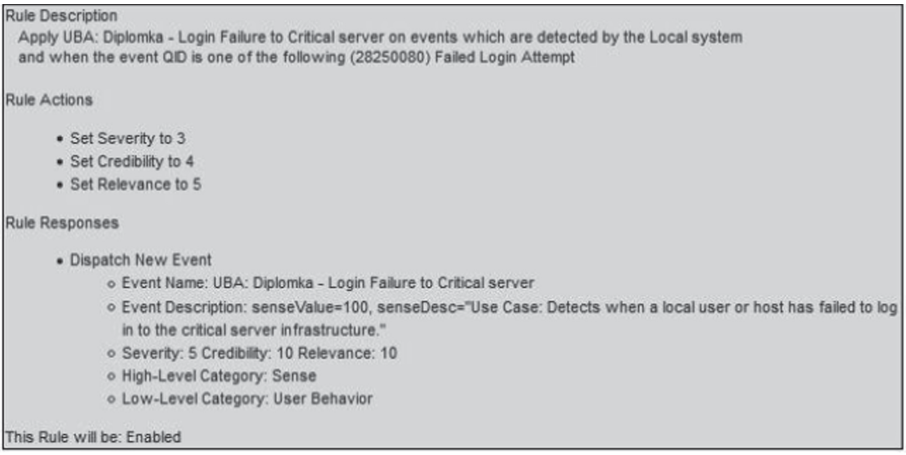

Fig. 3. QRadar rule detecting login failure. Source: authors

An unsuccessful user (username: jne) login event was invoked to test the rule created. This activity was detected by the rule and the risk score was increased by the user according to the parameters defined in the rule.

In the user activity schedule there is apparent an increase in the sense score associated with login failure activity and related activities that were invoked along with the login failure activity. The end result of the entire use case is the generation of a security incident pointing to the very risky behavior of the user.

Logrhythm

The AI Engine module was used to create the correlation rule. Figure 4 shows a preview of the correlation rule definition in the AIE module. The relational rule was set with the same parameters as the QRadar Use case. The rule is applied when an event specified as Authentication Failure is detected.

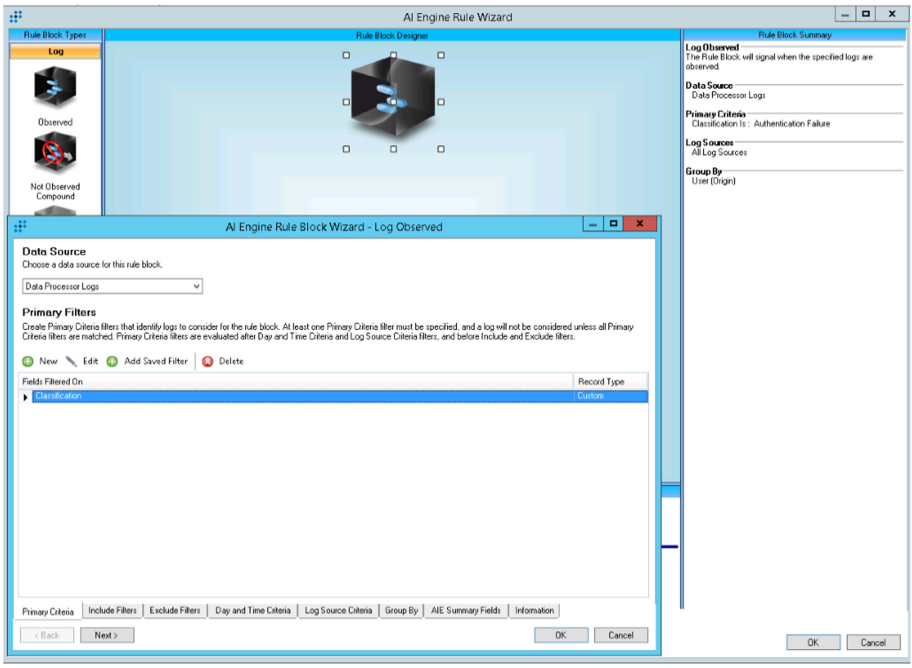

Fig. 4. LogRhythm - AIE definition of correlation rule. Source: authors

For the purpose of testing the rule created, an unsuccessful user login event has been invoked. This activity was detected by the rule just as in the case QRadar solution and the user's risk score was increased according to the parameters defined in the rule. As with QRadar, the detected activity is listed as well as related activities that were invoked along with login failure activity. Equally to the use of QRadar, the only output of the entire use case is the generation of a security incident pointing to highly risky behavior of the user.

4.2 Permission Delegation

The second case of using the UEBA module will be focused primarily on the problem that can be observed from time to time in the network infrastructure. It is an effort to include different users in groups that have a higher range of competences and are not subject to such extensive monitoring of their activities as they are expected to have a certain degree of security risk knowledge. Monitoring is also performed when attempting to

delegate permissions to users who do not have access to an administrator account or use an account without administrator privileges.

To detect this activity, a rule has been created that monitors activity on the domain controller. If an activity is detected that records an event of adding or removing a user to a security group, when a user who has performed this activity does not have administrator privileges, a security incident is generated to indicate that. The rule was created as well as in the case of the first Use-Case, via the QRadar installation wizard (Fig. 5).

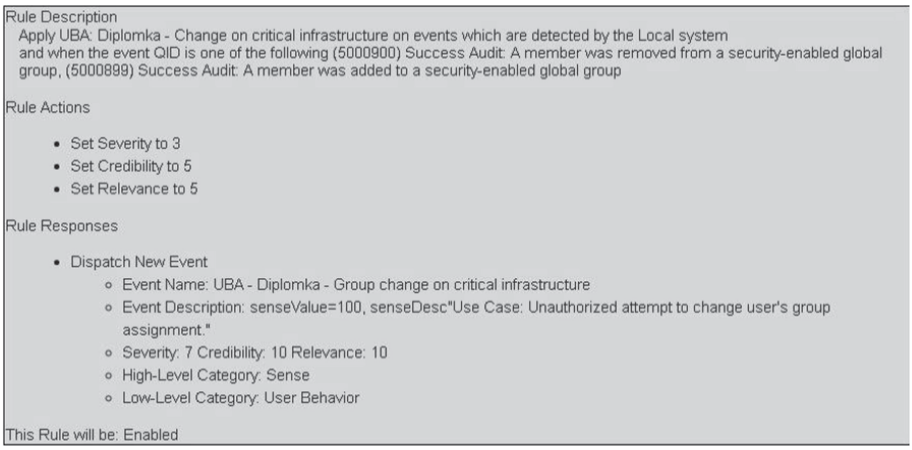

Fig. 5. QRadar - create a rule. Source: authors

After creating the rule, an action was taken to add a normal domain user to a domain administrator group that had been performed by the user. Based on the detected event, the risk score was increased by the user.

LogRhythm

The AI Engine module was used to create the correlation rule. For a relational rule was set with the same parameters as in the case of QRadar Use case. Figure 6 shows a preview of the correlation rule definition in the AIE module. The rule is applied when a received event related to a change of groups is detected in which the user is assigned and this activity is not performed by someone with administrative authority.

After creating a valid rule, an action to add a normal domain user to the domain admin group was made by the user. This activity was detected by the rule created, and the user's risk score was immediately increased, which was immediately visible in application. Same as in the case of the use, QRadar is the only output case of the entire use case of generating a security incident pointing to highly risky behavior of the user.

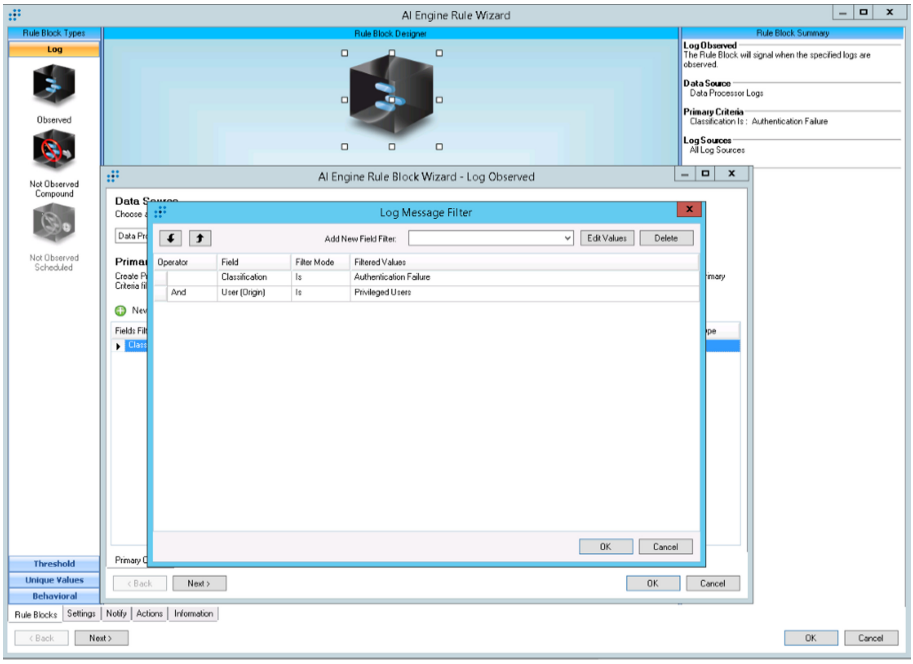

Fig. 6. LogRhythm - create a correlation rule. Source: authors

5 Conclusion

The aim of this article was to perform a comparative analysis of SIEM solutions emphasizing modules of user behavioral analysis in SIEM systems and their utility in cyber security energy systems. First, the issue of security in the area of energy systems was introduced with the possibility of using SIEM solutions for monitoring activities. In the following part of the article the general architecture of selected SIEM solutions was introduced, which are currently relevant to deployment in energy systems. Altogether three solutions were chosen for comparative analysis: AlienVault, IBM Security QRadar and LogRhythm NextGen SIEM. At the same time, general principles of user behavioral analysis were introduced emphasizing implementation options in selected SIEM solutions.

In the last part of the article, modules of user behavioral analysis were tested on two defined Use-Case emphasizing the possibilities of defining these Use-Case in SIEM solutions and detection of activities that have been invoked in Use Case testing.

In the case of the solution AlienVaultu OSSIM/USM, there was no separate UBA module used for collecting and evaluating information as well as data and monitored users. This functionality was promised to be executed by one of the company's specialists prior to testing Use-Case. Because of the absence of the UBA module, it was not possible to test the defined Use-Case in AlienVault. Utilizing AlienVault in energy systems relative to legislative requirements on auditing logs is problematic because the basic version of the solution includes only the possibility of monitoring the data stream.

At UBA solutions within IBM Security QRadar there was possible to track detailed information about users, which were also applied machine learning models. UBA module QRadaru uses a set of built-in use cases to solve problematic behavior, which can be extended by any custom use case. Defined Use-Case has been successfully deployed to QRadar solutions and their end result has always been manifested by the emergence of a security incident highlighting a potential threat in the infrastructure.

Compared to LogRhythm Solution NextGen SIEM, IBM Security QRadar has the full functionality and licensing of UBA modules already the basic solution. In the case of deployment and use of UBA module in LogRhythm NextGen SIEM solution, as well as QRadar, it was able to track detailed user information, also including machine learning models. The defined Use Case was successfully deployed to LogRhythm by AI Engine and their final outcome was also always the emergence of a security incident highlighting the potential threat of the network infrastructure.

The principal and ultimate added value of the LogRhythm solution is the possibility of creating a so-called Use Case over relevant security incidents, possibly over a user-defined group of events. This includes the ability to add related activities to security incidents that are related to user activity, giving Use Case the ability to compile a detailed overview of the origin of activities and their impact on infrastructure.

Acknowledgment. This work and the contribution were supported by a Specific Research Project, Faculty of Informatics and Management, University of Hradec Kralove, Czech Republic. We would like to thank Mr. J. Nedbal, a graduate of Faculty of management and informatics, University of Hradec Kralove, for the practical verification of the proposed solutions and close cooperation in the solution.

References

1. Keyhani, A.: Design of Smart Power Grid Renewable Energy Systems. John Wiley & Sons, Hoboken (2016)
2. Zakeri, B., Syri, S.: Electrical energy storage systems: a comparative life cycle cost analysis. Renew. Sustain. Energy Rev. **42**, 569–596 (2015). https://doi.org/10.1016/j.rser.2014.10.011. ISSN13640321
3. Jarmakiewicz, J., Parobczak, K., Maślanka, K.: Cybersecurity protection for power grid control infrastructures. Int. J. Crit. Infrastruct. Prot. **18**, 20–33 (2017)
4. Aitel, D.: Cybersecurity essentials for electric operators. Electricity J. **26**(1), 52–58 (2013). https://doi.org/10.1016/j.tej.2012.11.014, ISSN 10406190
5. Peterson, J., Haney, M., Borrelli R.A.: An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. Nuclear Eng. Des. **346**, 75–84 (2019). https://doi.org/10.1016/j.nucengdes.2019.02.025, ISSN 00295493
6. LI, L., He W., Li XU, Ash I., Anwar M., Yuan X.: Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. Int. J. Inf. Manag. **45**, 13–24 (2019). https://doi.org/10.1016/j.ijinfomgt.2018.10.017, ISSN 02684012
7. Li, D., Guo, H., Zhou, J., Zhou, L., Wong, J.W.: SCADAWall: a CPI-enabled firewall model for SCADA security. Comput. Secur. **80**, 134–154 (2019). https://doi.org/10.1016/j.cose.2018.10.002.ISSN01674048
8. Rezai, A., Keshavarzi P., Moravej Z.:. Key management issue in SCADA networks: a review. Eng. Sci. Technol. Int. J. **20**(1), 354–363 (2017). https://doi.org/10.1016/j.jestch.2016.08.011.

9. Nazir, S., Patel, S., Patel, D.: Assessing and augmenting SCADA cyber security: a survey of techniques. Comput. Secur. **70**, 436–454 (2017). https://doi.org/10.1016/j.cose.2017.06.010.ISSN01674048
10. Makkar, A., Kumar, N.: User behavior analysis-based smart energy management for webpage ranking: Learning automata-based solution. Sustain. Comput. Inf. Syst. **20**, 174–191 (2018). https://doi.org/10.1016/j.suscom.2018.02.003.ISSN22105379
11. Yang, L., Wang, Y., Zhou, Y., Wang, J., Fan, Ch., Zhu, Ch.: OA user behavior analysis with the heterogeneous information network model. Phys. A Stat. Mech. Appl. **516**, 552–562 (2019). https://doi.org/10.1016/j.physa.2018.09.116.ISSN03784371
12. Raja, M., Niranjan S., Vasudevan A.R.: Rule generation for TCP SYN flood attack in SIEM Environment. Procedia Comput. Sci. **115**, 580–587 (2017). https://doi.org/10.1016/j.procs.2017.09.117, ISSN 18770509
13. Maher, D.: Can artificial intelligence help in the war on cybercrime? Comput. Fraud Secur. **2017**(8), 7–9 (2017). https://doi.org/10.1016/S1361-3723(17)30069-6.ISSN13613723
14. Nurmuhumatovich, J.A., Mikusova, M.: Testing trajectory of road trains with program complexes. Arch. Autom. Eng. Archiwum Motoryzacji **83**(1), 103–112 (2019). https://doi.org/10.14669/AM.VOL83.ART7
15. Krejcar, O., Frischer, R., Smart intelligent control of current source for high power LED diodes, Microelectron. J. **44**(4), 307–314 (2013). ISSN: 0026–2692, eISSN: 1879–2391