

Oleh IVANOCHKO¹, Oleh HARASYMCHUK², Vasyl RAMSH³

Opiekun naukowy: Oleh HARASYMCHUK²

ZASTOSOWANIE PLATFORMY IBM QRADAR SIEM DO WYKRYWANIA KRYTYCZNYCH ZAGROŻEŃ DLA CYBERBEZPIECZEŃSTWA

Streszczenie: Informacje na temat ważności zapewnienia bezpieczeństwa danych zostały omówione w artykule, na przykładzie użycia systemu SIEM. Opisano użytkowanie system IBM QRadar, a także scenariusz ataku hackerskiego oraz środki zaradcze (przeciwdziałania) terminu – sugerowane przez analityka bezpieczeństwa. Opisano jak je zaimplementowano i użyto.

Słowa kluczowe: ataki, zagrożenia, cyberzagrożenia, bezpieczeństwo, systemy SIEM, QRadar.

APPLICATION OF IBM QRADAR SIEM PLATFORM TO DETECT CRITICAL CYBERSECURITY THREATS

Summary: Information about the importance of ensuring information security is given using the example of SIEM systems. The operation of the IBM QRadar system has been demonstrated, and the scenario of an attack by an attacker and countermeasures by a security analyst has been developed and implemented.

Keywords: attacks, threats, cyber threats, security, SIEM systems, QRadar

1. Introduction

It is difficult to imagine the modern world without technologies, where every process, production, and even personal life of a person is connected with them. Today, information has become a commodity that can be exchanged, bought, or sold. Information becomes too valuable, sometimes even more valuable than the devices

¹ Lviv Polytechnic National University, student of Information Protection Department, oleg.ivanochkolenovo@gmail.com

² PhD, Lviv Polytechnic National University, Associated Professor of Information Protection Department, oleg.harasymchuk@gmail.com

³ PhD, Separated Subdivision of National University of Life and Environmental Sciences of Ukraine Berezhaný agrotechnical institute, Associated Professor of Energy and Automatics Department, ramsh_v@ukr.net

on which it is stored. As digital information processing devices improve, so does the number of possible vulnerabilities in the programs or physical devices that are created, as no perfectly configured system works flawlessly and is completely secure. As the demand for information grows, some individuals intend to find vulnerabilities in data transmission/storage/processing devices and gain unauthorized access to data, use it for their purposes, or destroy it altogether, thus causing damage. This also applies to large corporate networks where people work with large customer/resource bases. Every node in this network is a door for a criminal. Therefore, an integral part of information security is the control of these very "nodes", namely, keeping records of actions important for security (so-called "logs"), such as an attempt to log into the system, logging into the system, changing configurations, sending data via networks and others. It is for this purpose that there are software solutions created for the collection, analysis, and storage of logs - SIEM (Security Information and Event Management) systems [1-3].

Due to the phenomenon of worldwide globalization, the number of mega-corporations that own a large amount of their customers' data is growing, making them a target for criminals. Therefore, every corporation or business that works with a large staff of employees in the network needs to implement an SIEM - a system for the timely prevention of hacking attempts. Even if the data was still compromised, the SIEM system will help investigate this breach and reproduce all the steps taken by the attacker, which will help prevent similar attacks in the future [4-5]. With the growth of large companies, the number of logs that the SIEM system must process promptly also increases. Since the developers of SIEM systems are interested in optimizing the performance of the correlation core without increasing the physical resources of the system, and the number of cybercrimes is only increasing every year, SIEM systems will become even more relevant.

The purpose of the work is to research and analyze the operation of the information security management system and IBM QRadar SIEM information security events, to detect the actions of an attacker using this software..

2. An example of cyber threat detection using QRADAR SIEM

2.1. The main purpose and functions of SIEM systems

SIEM solutions that monitor information analyze security events in real-time that are received from network devices, information protection tools, IT services, infrastructure, and applications. SIEM systems are provided to providers as hardware devices, software or services, and applications for event collection and processing, notification, report generation, and visualization of IS violations. The composition and implementation of such components completely depend on the solution architecture, implementation size, performance parameters, and even the geographical location of the system.

The first task of a SIEM is to get data from the source. It can be both an "active" source that knows how to transmit data to the SIEM and is enough to specify the network address of the receiver and a "passive" one that the SIEM system must contact itself. After receiving data from the source, the SIEM system transforms them into the same format suitable for further use - this is called normalization. It can be compared

to a large company of people from different countries: everyone speaks their languages, and the SIEM system listens and normalizes everything, that is, translates everything into English, so that you can then review the entire conversation in a single language that everyone understands.

Next, the SIEM system performs taxonomy, that is, it classifies already normalized messages depending on their content: which event indicates successful network communication, which - about the user's login to the PC, and which - about the activation of the antivirus. Thus, not just a set of records is obtained, but a sequence of events with a certain content and time of occurrence.

Then the main mechanism of SIEM systems comes into play: correlation. Correlation in SIEM is a correlation between events that meet certain conditions (correlation rules). An information security incident is formed as a result of the activation of the correlation rules in the SIEM system (in some systems, for example, in SIEM IBM QRadar [1-6], the incident is called Offense). At the same time, the IS specialist when working with SIEM should be able to quickly search through the previous incidents and events stored in the SIEM system in case he needs to learn any additional technical details to investigate the attack.

An example of where a general SIEM receives data is shown in Figure 1.

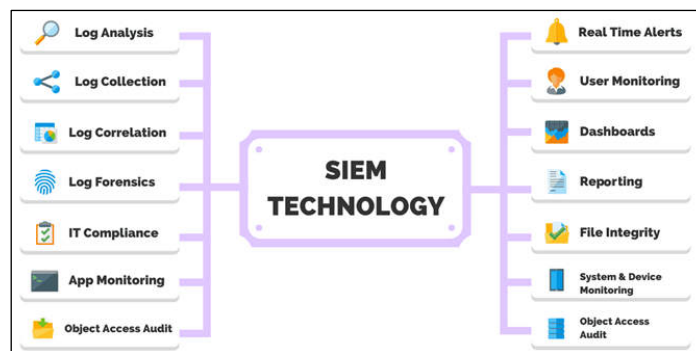


Figure 1. SIEM data sources

It is also worth adding that SIEM systems are intended only for monitoring and responding to incidents, and they do not allow for protection against threats or prevent them.

It can be said that without SIEM, no complex information security system can function.

The first task of a SIEM is to log security incidents in real time. The sooner the analyst receives notification of the incident, the sooner he can take certain measures.

The second task is to provide a convenient toolkit for retrospective analysis of security incidents and their investigation. All data presentations should be completely readable, easy to understand, and logically organized.

A properly configured SIEM is the brain of an information security system, but training this brain requires a very high level of specialist knowledge and well-defined IS processes.

In an ideal situation, the more event sources there are, the less likely it is to miss an important security event and fail to identify a significant incident, resulting

in a so called False Negative of the second kind, which sounds otherwise like an "undetected threat."

But practice suggests that with very large flows of events, the probability of errors of the first kind, False Positive, in turn, increases. Processing a large amount of data in a short period leads to the complication of the task of writing complex correlation rules and filtering processes that will handle these same errors. Not to mention that handling additional events can seriously add to the price of a SIEM solution.

Sometimes best practices recommend limiting the volume of events by filtering them by severity and specific source modules (facility). Such techniques are specifically used to preserve the performance of the SIEM system since not everyone can afford large capacities.

2.2. Comparative characteristics of modern SIEM systems

Let's consider modern SIEM solutions using the example of IBM QRadar, LogRhythm, and Splunk and their differences.

Table 1. Comparative of modern SIEM systems

Characteristic	IBM QRadar	LogRhythm	Splunk
<u>Strategy</u>	IBM has a wide internal resources and partnerships for support sales, deployment and operational support, including managed services for QRadar, in different geographical regions.	LogRhythm offers the only provider-ecosystem approach for buyers who want a unified decision that includes main SIEM, monitoring networks, monitoring endpoints, and UEBA.	Splunk's approach to granting centralized collection and analysis of data from premium decisions based on the main product turns to organizations that want one decision that may support several commands.
<u>Basic functions</u>	IBM QRadar is used for data analysis logs and network flows in the mode real-time, to malicious actions it was possible to discover and stop as soon as possible.	It is used for construction generally corporate systems detection and response to a threat.	Analyzes formed on machine data for software operational intelligence.
<u>Components</u>	QRadar offers users wide options in architecture deployment with a selection of factors, which can be deployed in different combinations Here include physical and virtual devices that can	LogRhythm has wide set options for launching the main SIEM solution, including physical equipment, software provision(for installations locally or in IaaS such as AWS,	Multiple implementation options for Splunk Enterprise and Enterprise Security include software, cloud host, and auxiliary devices.

	be All-in-one and separate components, also, bring your license for cloudy deployment.	Azure and Google Cloud) and SaaS.	
<u>Event processing</u>	Event data and stream data are processed on an All-in-One device without the need to add event processors or processor flow.	For processing events use collection device data and software.	Splunk uses data and indexes them, turning them into objects that can be searched in the form of events.
<u>Collection of incidents</u>	Qradar translates or normalizes the raw data in IP addresses, ports, number of bytes and packages and others information in stream records that represents a session between two hosts.	Collection of incidents takes place to help deploy LogRhythm, which unites the entire history of the event safety and determines sequence attacks.	By using Incident Review collects all incidents. After that significant events and their status are displayed.
<u>Correlation</u>	QRadar console processes data only against the rules specified in the historical profile correlation.	AI Engine LogRhythm carries out correlation of all types of activities.	Splunk supports five types of correlations -based on time and geographical coordinates, -based on transactions, -under search, -search, -accession.
<u>Visualization</u>	Tabular visualization with many tabs, conveniently divided into separate fields.	Convenient color visualization in the form of diagrams, graphs, schemes and tables.	Mainly tabular colored visualization for many additional sensors, windows, and statistics.
<u>Pricing policy</u>	IBM demonstrates more and more dependence on their additional products, available for additional costs, such as Resilient and QRadar Advisor for opportunities response to incidents	Everything with LogRhythm is expensive and nothing is not received free. LogRhythm sells a window which has a certain capacity for incoming log messages. After exceeding this containers to you will have to buy another box and cluster it.	Pricing is available as an eternal or annual license, based on the maximum daily data usage and starts from 2000 dollars per year for 1 GB / day. Splunk ES pricing intended for unlimited users for use of all data that relate to safety, for the solution of all cases using security.

<u>Customer experience</u>	It is necessary to improve analytics and QRadar behavior, as well as processes sales/contracting contracts supplier.	Customers LogRhythm Offer generally positive reviews about opportunities for the product.	Splunk customers give high marks for ease of integration, quality, and accessibility for end-user training, and the quality of the peer community compared to their competition.
-----------------------------------	--	---	--

So, after reviewing the comparative analysis, we can conclude that each manufacturer's system has its characteristics and advantages.

Instead, the QRadar complex provides a high level of scalability and productivity, centralized management, the possibility of configuration and adaptation to specific requirements based on service masters, and other benefits.

The main advantages of the application of IBM QRadar are increasing the level of security of the information infrastructure as a result of prompt response to information security incidents; acceleration and automation of the identification process, as well as further investigation of incidents; centralized an approach to the tasks of processing and storing information security events.

2.3. Overview of QRadar SIEM

IBM QRadar® Security Information and Event Management (SIEM) is designed to provide security teams with a centralized view of events across the enterprise and to properly prioritize those events for the fastest possible security decisions and actions. As a first step, this SIEM solution virtually ingests large amounts of data from all company endpoints and provides a comprehensive view of activity across on-premises and cloud environments. While processing the data, QRadar shows the threats in real time and prioritizes them based on the created rules and intelligent intelligence data. Actionable alerts provide greater insight into potential incidents, allowing security analysts to respond quickly and limit the actions of attackers. Unlike other solutions, QRadar is specifically designed to reference best practices with easy scalability and low effort to configure [6].

This solution includes more than 450 pre-built device support modules (Device Support Modules (DSMs)) that provide fast integrations with ready commercial technologies. Customers can simply send logs to QRadar, and the SIEM solution itself will automatically identify the source type and apply DSM to parse and normalize incoming data quickly. The result is that with QRadar, customers can work with data much faster than with other solutions. An additional advantage is the ability to install new integrations through a special application center "IBM Security App Exchange". Figure 2 shows where all this data comes from in QRadar SIEM.

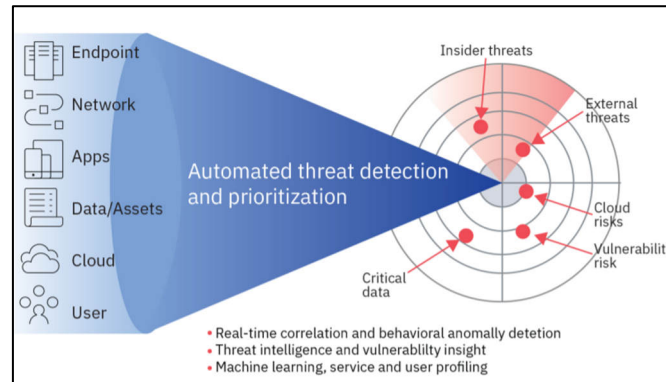


Figure 2. Sources of data sent to QRadar

QRadar includes a variety of anomaly detection capabilities to better identify changes in behavior that may be indicators of an unknown threat. The unique ability of this solution allows you to monitor and analyze the traffic of applications that operate at the 7th level of OSI. This allows for more accurate detection of anomalies than is the case with other SIEM solutions.

QRadar provides transparency, accountability, and measurability. These three points are essential to a company's success in meeting standards. The solution's ability to correlate and integrate threat information helps provide a more complete picture of IT risk reporting to auditors. Hundreds of ready-made reports and rule templates also facilitate faster compliance with standards.

2.4. Practical cyber threat detection with QRadar SIEM

Working with the received data can be quite a difficult task. Every second, thousands of activity logs are received in the centralized system, and not every system can cope with such a flow of data. In order not to overload the analysis systems, you must first configure the correct collection of logs.

For the most part, for small companies, standard settings for system audits are used, which are configured in GPO (Group Policy Object). GPOs are a tool available to administrators who configure Active Directory architecture. It allows you to centrally manage settings on domain-joined client computers or servers, and quickly distribute software.

During the test, all actions were pre-agreed and performed on real systems that guarantee the safety of employees in the company.

The first implemented attack scenario is simple. The attacker is trying to gain unauthorized access to the system administrator account where the company's two-factor authentication settings console is located. To do this, he must use the "brute-force" password selection technique.

The method of selecting passwords allows an attacker to quickly select the correct login data for user accounts with the help of utilities that automate the entire process. Brute-force is currently one of the most popular methods of cracking passwords to user accounts of any service.

First, the attacker conducts reconnaissance, which helps to find out which users are administrators in the internal systems of companies. After the required information has been obtained, he enters the systems and searches for login forms.

In the scenario to prevent such an attack, the security analyst should analyze the activity logs coming from the two-factor authentication administration panel in advance and configure a rule that will count the failed login attempts to the admin panel: "If in the last 5 minutes, there were at least 5 failed login attempts to the panel administrator (for this event there is a special identifier that is recognized by the QRadar solution), then you need to create a security alert." In fig. 3-4 shows the configuration of this rule in the QRadar system.

After the SIEM solution detects these unsuccessful login attempts, an "Offense" will be generated with the corresponding name "Authentication: DUO admin console multiple unsuccessful logins".

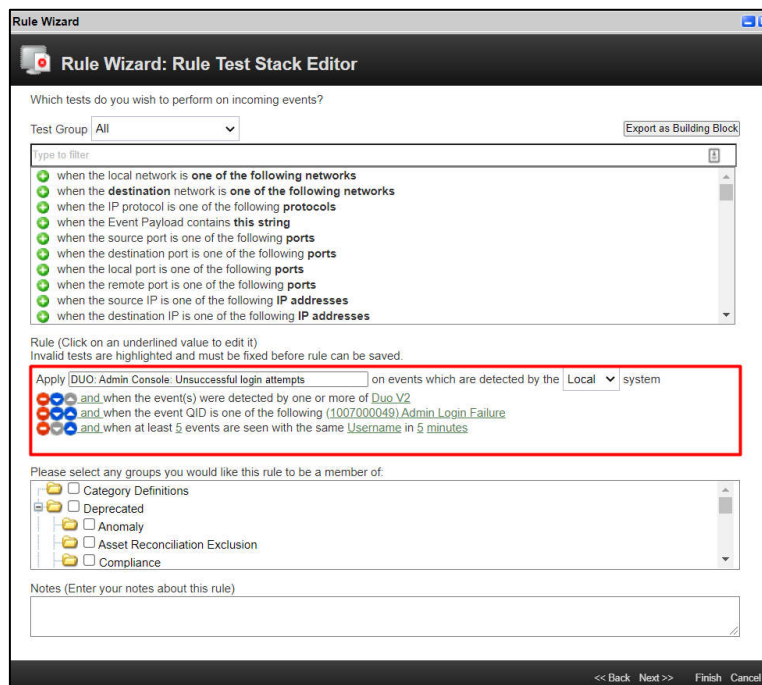


Figure 3. Creating rule logic

Figure 4. Creating an action that will send a security alert

After going to the "Offenses" tab, where all security breach notifications are collected, the security analyst sees that a security notification has arrived that indicates the brute force that was created by the script (Fig. 5).

ID	Description	Offense Type	Offense Source
38540	Impact: 2 Urgency: 2 Group: EPAM - IT Security Emerg: 0 Title: [SOC] Offense ID:xxxx EPAM: Authentication: DUO admin console multiple unsuccessful logins	Username	p34h...1vets:1w07B...
37076	File Location Disconnect	Source IP	10.66.110.226
37075	File Location Incorrect	Source IP	10.253.0.42
37072	Impact: 1 Urgency: 1 Group: EPAM - IT Security Emerg: 0 Title: [SOC] Offense ID:xxxx EPAM: SIEM: BSS server stop sending logs (Project)	Source IP	10.245.237.41
37074	Impact: 1 Urgency: 2 Group: EPAM - IT Security Emerg: 0 Title: [SOC] Offense ID:xxxx EPAM: SIEM: Backup Issue	Source IP	10.240.0.241
36598	Impact: 2 Urgency: 1 Group: EPAM - IT Security Emerg: 0 Title: [SOC] Offense ID:xxxx EPAM: Potential Infection: S1 detected threat on critical group asset	Threat ID (custom)	1158100200260241902
35507	Impact: 2 Urgency: 1 Group: EPAM - IT Security Emerg: 0 Title: [SOC] Offense ID:xxxx EPAM: Potential Infection: S1 detected threat on critical group asset	Threat ID (custom)	1158100200260241902

Figure 5. Notification that the administrator's account is being hacked

The next action of the analyst is to investigate. Double-click on the message to open more detailed information about the events. In Fig. 6, you can see the open message, and it contains information about who is the victim of the attack, from which IP address it is taking place, and how many times the attacker tried to log into the account.

The screenshot displays a security breach message for 'Offense 38540'. The interface includes a navigation bar at the top with options like 'Activity', 'Network Activity', 'Assets', 'Reports', 'Admin', and 'Palo Alto Networks'. The main content area shows the offense details, including a progress bar for 'Magnitude', a 'Description' of 'Impact: 2 | Urgency: 2 | Group: EPAM - IT Security | Emerg: 0 | Title: [SOC] Offense ID:xxxx EPAM: Authentication: DUO admin console multiple unsuccessful logins', and 'Source IP(s)' 10.245.128.161. A table titled 'Offense Source Summary' lists fields such as Username (oleh.i.vanochko87@epam.com), MAC Address, Last Known Host, Last Known MAC, Last Observed, and Offenses (8). The 'Actions' menu is open, showing options like 'Follow up', 'Hide', 'Protect Offense', 'Close', 'Email', 'Add Note', and 'Assign'.

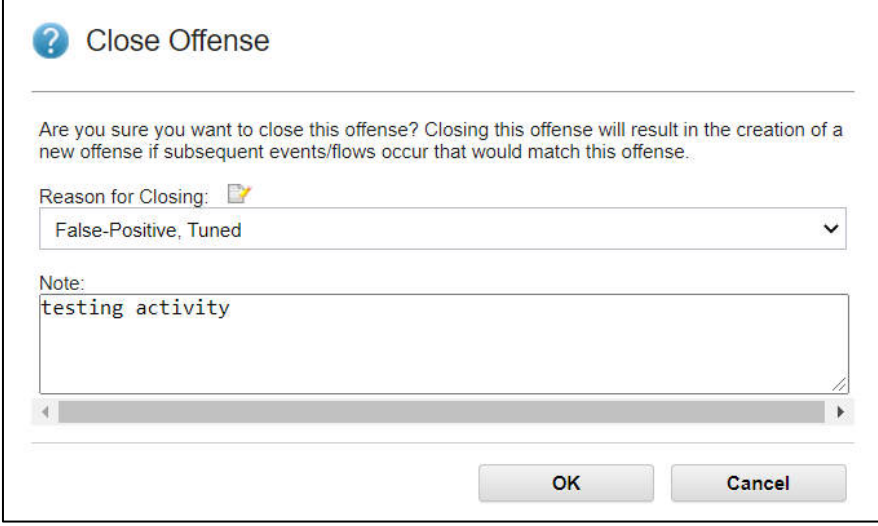
Figure 6. View of a security breach message

After taking appropriate actions, such as blocking the IP address from which the attack is taking place, the security analyst can "close" the incident by clicking on the "Actions" and "Close" buttons, respectively (Fig. 7).

This screenshot shows the same 'Offense 38540' details as Figure 6. The 'Actions' menu is open, and the 'Close' button is highlighted with a red circle, indicating the next step in the process of closing the incident.


Figure 7. Closing the incident

Next, in the context menu, you need to select the reason for closing and write an additional explanatory comment. False-Positive is chosen, since this activity in our case is only a simulation of an attack (Fig. 8). Also, in addition to False-Positive (an error of the first kind), there are such options as: "policy violation", "is not a security problem", "testing rule" in the reasons for closing.



? Close Offense

Are you sure you want to close this offense? Closing this offense will result in the creation of a new offense if subsequent events/flows occur that would match this offense.

Reason for Closing:  False-Positive, Tuned

Note:
testing activity

OK Cancel

Figure 8. Selecting reasons and writing a comment before closing the incident

In this way, we show how the IBM QRadar SIEM system receives logs, processes them and, with the help of configured security rules, detects anomalies and creates notifications for security analysts about violations.

It was developed and implemented attacker scenarios and security analytics. On the part of the attacker, a "Brute Force" attack was carried out on the web panel of the two-factor authentication administration, and on the part of the analyst, a rule was developed that detected the attack and sent a security alert.

After the experiment and the obtained results, it was concluded that the IBM QRadar SIEM solution copes well with the tasks of constant monitoring of the company's activities.

Therefore, the correct setting of log collection is a guarantor of the effectiveness of detecting anomalies and threats to the company's security. The company should have a separate department for information protection and a working SIEM system. Security teams must properly configure the relationships between the components of SIEM solutions as required by the architecture itself.

3. Conclusions

The paper considers the use of SIEM solutions to guarantee security in corporate networks. Based on reviewed literary sources, expert opinions of leading specialists in the IT industry, and statistical data, the relevance of the topic has been established. Analyzed SIEM systems as an additional and very important element of protection against targeted attacks in which the system detects an intrusion. Data collection and event processing in modern SIEM systems and their comparative characteristics are studied.

Based on the results of a comparative analysis of existing solutions in the market of SIEM systems, IBM QRadar was chosen. An analysis of the characteristics, features of work, and sources of information with which this SIEM system works has been carried out. The description of its operation, architecture, and appearance of the console is considered. Here are some examples of what data IBM QRadar can accept. In the example of the work of this modern SIEM system, work with security incidents is demonstrated, as well as how to counter and investigate the attempts of a possible attacker to attack the corporate network. Reports and statistics of all events that occurred in the system are provided. Demonstrated successful detection of a web application attack using customized rules.

REFERENCES

1. GRANADILLO G., GONZÁLEZ-ZARZOSA S., DIAZ R.: Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures (2021). *Sensors*. 21. 4759. 10.3390/s21144759.
2. Alienvault, "The SIEM Evaluator's Guide," AlienVault, Tech. Rep., 2022. [Online]. Available: <https://cdn-cybersecurity.att.com/docs/guides/The-SIEM-Evaluators-Guide.pdf>
3. VIELBERTH M.: Security Information and Event Management (SIEM), in *Encyclopedia of Cryptography, Security and Privacy*, Mar. 2021.
4. KARRI YASWANTH: Detection of DoS attack and Zero Day Threat with SIEM (2023). 10.13140/RG.2.2.28359.78248.
5. AL-DUWAIRI, BASHEER, WAFAA AL-KAHLA, MHD AMMAR ALREFAI, YAZID ABEDALQADER, ABDULLAH RAWASH, RANA FAHMAWI. SIEM-based detection and mitigation of IoT-botnet DDoS attacks. *International Journal of Electrical and Computer Engineering (IJECE)* (2020).
6. GUNDER A.: Security monitoring and management based on the use of the IBM QRadar SIEM system. *Modern Information Security*. 2(2022). 10.31673/2409-7292.2022.020614.