DOI: 10.2507/34th.daaam.proceedings.014

COMPARATIVE ANALYSIS OF IBM QRADAR AND WAZUH FOR SECURITY INFORMATION AND EVENT MANAGEMENT

Dario Šuškalo, Zlatan Morić, Jasmin Redžepagić & Damir Regvart

This Publication has to be referred as: Suskalo, D[ario]; Moric, Z[latan]; Redzepagic, J[asmin] & Regvart, D[amir] (2023). Comparative Analysis of IBM Qradar and Wazuh for Security Information and Event Management, Proceedings of the 34th DAAAM International Symposium, pp.0096-0102, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-41-9, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/34th.daaam.proceedings.014

Abstract

The objective of this paper is to conduct a comparative analysis between two prominent SIEM tools: the commercial IBM QRadar SIEM and Wazuh, an open-source security solution. The chosen focal point was to assess the extent to which these tools can meet the security requirements within a typical IT infrastructure. The selection of this paper aimed to evaluate the efficacy of these tools in addressing the security needs prevalent in contemporary IT setups. The practical phase of the research was built around carefully curated scenarios that mirror the daily security incidents encountered by businesses. This deliberate choice was underpinned by the significance of understanding how QRadar and Wazuh interpret and respond to such events.

Keywords: SIEM; QRadar; Wazuh; event management.

1. Introduction

Systems for managing security information and events in the information system, or SIEM (Security Information and Event Management) systems are created to serve as a central place where all devices in the computer system forward their log records. SIEM systems [1][2] enable real-time monitoring, analysis and correlation of security events in the IT system, thus giving computer security experts better visibility into what was really happening within the system during and after a security incident.

This paper describes the working principle of the SIEM system in general, and then analyzes two different solutions - the commercial IBM QRadar system [3][4] and the open source Wazuh system [5] [6]. In the realm of commercial software, the manufacturer's access to the solution's underlying code is typically restricted to the development engineers who created the system. This proprietary nature renders the solution the intellectual property of the company, and end-users are required to procure licenses for utilization. Conversely, open-source solutions embody a contrasting ethos. They are freely accessible to all interested users, as the developers who conceptualized such solutions opt to share the source code for examination, modification, enhancement, and even redistribution. The main point of this analysis lies in the meticulous evaluation of both products, discerning the respective merits and drawbacks inherent in each solution.

The investigation seeks to ascertain whether these systems hold the capacity to effectively cater to the requisites of a conventional IT environment. Beyond this, the research scrutinizes whether one solution exhibits functionalities absent in the other, and whether these specific attributes carry critical implications for bolstering system security. At the heart of this examination is a paramount consideration: the financial rationale behind investing in QRadar.

In essence, this study operates as a discerning compass navigating through the intricate landscape of SIEM solutions. By assessing the tangible strengths and limitations of IBM QRadar and Wazuh, it aims to unravel not only the viability of these systems within a typical IT framework but also the delicate equilibrium between investment and returns in the context of QRadar. Through this exploration, a more comprehensive understanding of these solutions and their applicability in diverse scenarios emerges, aiding decision-makers and IT professionals in shaping their cybersecurity strategies.

2. Background and Theoretical Framework

SIEM systems have emerged as indispensable components of modern cybersecurity strategies. These systems play a pivotal role in aggregating, correlating, and analyzing vast volumes of security data generated by various network and system components. Their overarching goal is to provide organizations with the ability to identify and respond to potential threats in real-time, enhancing the overall cybersecurity approach. A SIEM system combines security information management (SIM) and security event management (SEM) functions. SIM involves the collection, normalization, and storage of security-related data, while SEM revolves around real-time event correlation and threat detection. Companies often have problems with the security of their IT systems because they do not have complete visibility of what is happening within their network.

This happens for several reasons:

- There is no system for detecting anomalies or abnormal activities;
- Lack of insight into events on end users computers;
- Too many different tracking tools that are not integrated;
- Oversaturation with the amount of log entries;
- Higher cost of security management and maintenance;
- Inefficient enforcement of compliance policies within the system;
- Lack of resources or employee skills to interpret security events.

2.1. QRadar: Commercial model

QRadar is a robust and commercially available SIEM solution developed by IBM. The solution offers advanced threat detection and incident response capabilities, utilizing machine learning and behavioural analytics to identify deviations from normal behaviour. The solution's commercial nature entails proprietary software and a licensing model, allowing IBM to tightly control access to its source code. The system has a modular architecture, so that it would enable the visibility of the IT infrastructure, and it is scalable to meet the needs of the end users.

The components of QRadar include:

- Event and Flow Processors - responsible for collecting raw event and flow data from various sources, including network devices, servers, applications, and endpoints
- Data Nodes - store the processed and normalized data, usually distributed across the network to ensure high availability and reduced latency
- Event and Flow Collectors - collects the events from intermediate devices via SPAN (Switchport Analyzer) port to Event and Flow Processors
- QRadar Console - user interface for management and event monitoring
- QRadar Risk and vulnerability Manager - assistant for visualization of network topology and identifying vulnerabilities and misconfigurations.
- App Framework- allows integration of third-party applications and extensions.

Its distributed nature, advanced analytics, and customizable features make it a powerful solution for organizations seeking robust SIEM capabilities.

2.2 Wazuh: Open-Source Model

Wazuh represents an open-source approach to SIEM. It is built on the Elastic Stack and is tailored for extensibility and customization. Wazuh not only gathers and analyses security data but also provides intrusion detection, vulnerability detection, and compliance monitoring. The open-source nature of Wazuh encourages community participation, enabling collaborative development, and transparent code accessibility.

Some of the key advantages of the system are:

- Security analytics – the system collects, indexes and analyses security data that can be used to detect threats, unusual behaviour and intrusions into the organization's IT infrastructure.
- Intrusion Detection – The Wazuh system uses agents on the systems it monitors to detect malware and suspicious anomalies. The agent recognizes hidden files, processes, unregistered network connections, as well as unusual responses to system calls. The server component of the Wazuh system uses signature-based detection to detect intrusions into network nodes by analysing the collected log records.
- Analytics of log records – agents read the log records of operating systems and applications installed on a network node and forward them to a central manager where the records are analysed and stored. The system, using defined rules, enables system managers to detect problems more easily in applications or configurations, attempts to launch harmful operations, and violations of security policies.
- File integrity monitoring – The Wazuh system monitors the file system on a network node. Tracks changes to file permissions and ownership, as well as the users who made those changes. It is possible to combine file integrity data with threat data to identify compromised network nodes and security vulnerabilities.
- Vulnerability detection – Wazuh agents collect information about the software on the monitored nodes and send it to the Wazuh server where a comparison is made with the database of known CVE (Common Vulnerabilities and Exposures) vulnerabilities in order to identify vulnerabilities.
- Configuration assessment - by monitoring the configuration of systems and applications, compliance with defined security policies, rules or standards is ensured. Agents periodically scan monitored nodes for security risks within applications. If the Wazuh system detects deficiencies in the configuration, it sends recommendations on how to correct them.
- Incident Response – Wazuh provides proactive actions that need to be taken to combat detected threats, such as blocking access to threats. The system can also be used for computer forensics and incident response by remotely executing queries or commands and identifying indicators of compromise – IOCs.
- Regulatory compliance – the system provides measures to meet regulations, industry requirements and laws. Also, scalability and cross-platform support ensure compliance standards are met for organizations. Financial institutions and payment processing companies rely on Wazuh to comply with the regulations defined in the PCI DSS (abbr. Payment Card Industry Data Security Standard) standard, as well as additional supported regulations, such as GDPR (abbr. General Data Protection Regulation), NIST 800-53 (abbr. Security and Privacy Controls for Information Systems and Organizations) and HIPAA (abbr. The Health Insurance Portability and Accountability Act).
- Security monitoring of cloud services - using integration modules, security data from cloud services, such as Amazon AWS, Microsoft Azure or Google Cloud, is collected at the API level. It evaluates the system configuration, detects flaws and offers suggestions for improvement.
- Container security – the system provides visibility at the server level, as well as at the level of individual containers. Support for integration with Docker containers enables monitoring of network and storage configuration, as well as of the Docker container image itself.

3. Tools scenarios and analysis

In the experimental part of the work, a test environment consisting of several different virtual computers, as well as a firewall connecting the computers to the network, was set up. QRadar and Wazuh SIEM systems are installed in the working environment, inside LAN part of the network, which collect log records from all virtual devices, and thus monitor security events in the network. PC with Kali Linux OS presents the computer of a malicious user who is trying to hack into the system as seen in figure 1. The CI/CD toolset [7] was used inside test scenario.

Thorough documentation of IT processes is essential [8], as it serves as a critical asset in forensic investigations. These procedures play a crucial role in maintaining the investigation's integrity by providing a clear and unambiguous record of the steps taken during the investigative process. Documentation ensures that all actions, from the initial detection of an incident to the collection of digital evidence, are transparent, accountable, and in compliance with established protocols and legal requirements. Moreover, it aids in preserving the chain of custody, allowing investigators to demonstrate that evidence has not been tampered with or compromised. In addition to its significance in legal proceedings, comprehensive documentation is invaluable for knowledge transfer within an organization, enabling staff to learn from past incidents and continuously improve their incident response capabilities. Therefore, a well-documented IT process not only strengthens the credibility of forensic investigations but also contributes to the overall resilience and security posture of an organization.

3.1. Test-case Scenarios

Several scenarios were selected and the behaviour of both SIEM systems was observed, whether security events and threats are interpreted in accordance with the expected results [9].

The following scenarios were selected:

a) User activity

- User login to the system
- Attempt to change the password
- Changes to user accounts

b) Attacks with successive attempts (*brute-force*) on the remote access service
c) Attacks with successive attempts on the Outlook Web Access service
d) Apache web service scanner
e) Malicious attempts to access the network firewall

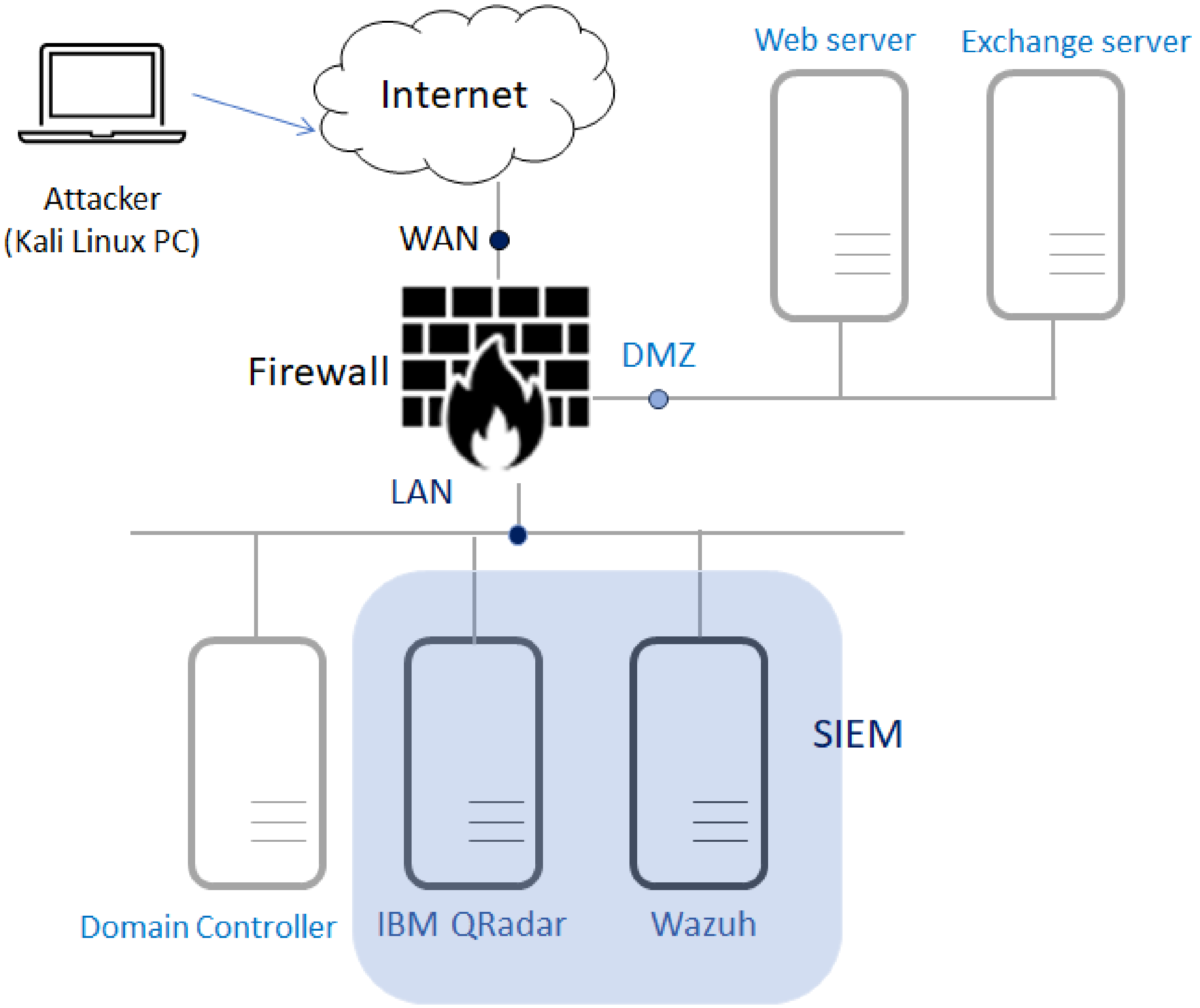

Fig 1. Test scenario topology

3.2 Comparative Analysis

The methodological approach enables to identify which solution excels in specific areas but also discern the nuanced differences that might be vital for organizations with unique security needs [10] [11]. Furthermore, it fosters an objective and evidence-based decision-making process, empowering organizations to select the SIEM solution that aligns most closely with their security goals and operational requirements. In a rapidly evolving cybersecurity landscape, where threats continually evolve, a rigorous comparative analysis is an indispensable tool for organizations striving to safeguard their digital assets effectively. The results of the test scenario are shown in table1.

Scalability is a hallmark of IBM QRadar. It is well-suited for large enterprises dealing with substantial data volumes. The architecture supports distribution, making it an optimal choice for organizations with complex and expansive IT environments. Wazuh also offers scalability, but it may necessitate more manual configuration in comparison to QRadar. This flexibility makes it adaptable to a range of organization sizes, from small to medium enterprises to larger institutions. While feature rich, QRadar can present a steeper learning curve. Efficient utilization often requires training and familiarity with its comprehensive interface. Wazuh distinguishes itself with a more straightforward setup and user interface. This simplicity can be attractive to organizations seeking rapid deployment and user-friendly management.

Scenario	QRadar analysis	Wazuh analysis	Conclusions
User Activity	The system has successfully detected: • Successful login • Unsuccessful login • Password change • Changes over user accounts		Using the machine learning component, QRadar intelligently groups individual events into chained violations. For example, if a user commits multiple unsuccessful reports, then makes a successful login, the system links these events to a violation that a system administrator can investigate.
			Wazuh does not have a machine learning component but is capable of detecting multiple low-level events and generating a higher-level event.
Attacks with successive attempts on remote access service	The system successfully detected successive unsuccessful attempts to log in to an SSL VPN service, and generated chained violations.	The system has successfully detected successive unsuccessful attempts to sign in to an SSL VPN service.	QRadar generated a chained foul.
			Wazuh generated an event of a significant level, but it was necessary to search the diary entries by key fields.
Attack on Outlook Web Access service	The system successfully detected an attack on the OWA service, created a chained violation from three different types of journal entries	The system successfully detected an attack on the OWA service, generating individual Level 5 events, and Group Events of Level 10.	QRadar has generated a chained breach that shows that the event is significant and requires further investigation.
			group events, which can bring attention to system managers for investigation.
Apache web service scanner	The system detected the scanner, however it did not create a violation, because the scanner itself tries to detect if there are certain files on the web server.	The system detected the scanner and created individual events, as well as group events of a more significant level.	QRadar did not create a violation, so this event would go unnoticed.
			Wazuh created a group event of a significant level, so such a security incident would attract the attention of security experts.
Malicious attempts to access a network firewall	The system detected many unsuccessful attempts to access the Fortigate system through the SSH protocol, and created multiple chain violations that would be immediately spotted and investigated by system managers.	The system detected a large amount of individual unsuccessful access attempts and assigned Level 5.	QRadar created multiple chained violations, and system managers would immediately notice unusual activity.
			Wazuh also recorded a large number of events, but given the events are not grouped, there is a chance that the attack would go unnoticed if it did not last for a long period of time.

Table 1. Comparative Analysis of IBM QRadar and Wazuh

IBM QRadar receives updates to DSMs, protocols, and decoders on a daily base, as IT equipment manufacturers are constantly developing new hardware and software. IBM also has an IBM Security App Exchange store with extensions that are mostly free for users who own a QRadar license.

The applications placed in this store are developed in cooperation with other manufacturers of security equipment, so they are compatible with QRadar and do not require complex installation. The following example is a real-life example: Cisco released Firepower Management Center (abbr. FMC) version 7.0 earlier this year. The commercial IBM QRadar system in use had the Cisco eStreamer extension installed that could read and decode network streams from Cisco FMC up to version 6.5. As the new version was released, at one point the FMC was updated from version 6.5 to 7.0 and after that it was noticed that the eStreamer function does not work, that is, that QRadar no longer receives records of network streams from the FMC. After spending some time researching, the problem was reported to IBM support. It was reported back that they currently do not support eStreamer for FMC 7.0, but that they will soon rework the extension to support it. Functionality was restored within a month. This kind of problem would not be solved in such a short time by the Wazuh developers for the simple reason that it is an open-source system.

Utilizing Wazuh as a SIEM solution offers significant advantages. Wazuh benefits from a passionate and community-driven development team, driven by their enthusiasm and a commitment to contributing to the broader community. A practical example that highlights this communal spirit pertains to the redirection of network logs from a Fortigate network device to Wazuh. During this process, it became evident that the built-in decoders within Wazuh were outdated, causing inaccuracies in log interpretation. Fortunately, the open-source ethos of Wazuh led to a solution. A diligent online search unearthed a decoder crafted by an altruistic individual who voluntarily shared the code with the wider community, without any expectation of payment or reservation. Their sole motivation was to aid the advancement of the Wazuh tool. Another real-world scenario involved redirecting VPN connection logs from virtual Cisco ASAs (network firewalls) to a production Wazuh SIEM. The integrated decoder in this case proved inadequate in interpreting log records from these virtual ASA devices, misinterpreting them as logs from much older Cisco PIX firewalls that have long been out of production. Again, the power of online collaboration came to the rescue as a suitable decoder was sourced from the internet, adept at accurately interpreting records from these virtual network devices, effectively resolving the issue.

4. Conclusion

Both systems successfully cope with the detection of security incidents presented through the previous scenarios. QRadar and Wazuh can be installed as single and distributed appliances and can cover multiple geographic locations at once. They have similar additional functionalities that can expand their role as security tools. If a company has a complex IT infrastructure, covers dozens of locations, has a large budget for procuring security solutions and resources for setting up multiple hardware-demanding devices, often acquires new IT equipment and needs timely support, it should choose IBM QRadar as its SIEM solution. If the company is smaller, has a limited budget and resources, and relies on the open source community to use or even develop its own solutions, then it is definitely recommended to implement Wazuh SIEM as a security solution. And there is always a compromise solution: using an IBM QRadar system with some basic license that can cover critical infrastructure that needs timely support, while for less essential systems, Wazuh or another open source SIEM can be used.

- IBM QRadar excels in terms of comprehensive security features and scalability, making it suitable for large enterprises with robust security requirements.
- Wazuh offers a cost-effective open-source solution with a user-friendly interface, making it accessible to a wide range of organizations.

The choice between IBM QRadar and Wazuh hinges on an organization's specific security needs, budget considerations, and the level of customization and support required [12]. This comparative analysis aims to provide a foundation for informed decision-making in selecting the most appropriate SIEM solution.

In future works, other SIEM solutions, whether they are commercial or community-driven, can also be used for comparison using the user scenarios and methodology described in this study. This approach can open the possibility of creating a broader comparative framework, allowing organizations to evaluate a more extensive array of SIEM options available in the market. By applying the same user scenarios and rigorous methodology, organizations can make more informed decisions when selecting the SIEM solution that best aligns with their unique security requirements and constraints. Furthermore, this expansion of the comparative analysis can contribute to the ongoing advancement of the field of cybersecurity, fostering a deeper understanding of how various SIEM solutions perform in real-world scenarios and promoting the development of more effective and resilient security strategies.

5. References

[1] Gustavo, G.G.; González-Zarzosa, S. & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures, Sensors 21, no. 14: 4759. https://doi.org/10.3390/s21144759

[2] Miller, D.R.; Harris, S.; Harper, A.; VanDyke, S. & Blask, C. (2010). Security information and event management (SIEM) implementation. McGraw Hill Professional., Default Book Series. October 2010, DOI: 10.1036/9780071701082

[3] https://www.IBM.com/community/qradar/wp-content/uploads/sites/5/2020/11/b_qradar_community_edition_7.3.3GA_v1.0.pdf (2021). IBM QRadar Community Edition 7.3.3, Access: 2023-03.

[4] https://www.IBM.com/docs/en/qsip/7.3.3?topic=SS42VS_7.3.3/com.IBM.qradar.doc/c_qradar_pdfs.html (2021). IBM QRadar SIEM V7.3.3 documentation, Access: 2023-03

[5] https://documentation.wazuh.com/current/getting-started/components/wazuh-agent.html (2021). Wazuh agent - Components · Wazuh documentation, Access: 2023-05

[6] https://documentation.wazuh.com/current/getting-started/architecture.html (2022). Architecture - Getting started with Wazuh · Wazuh documentation, Access: 2023-05

[7] Dakić V.; Redžepagić J.; Bašić M. (2022). CI/CD Toolset Security, 33rd DAAAM International Symposium on Intelligent Manufacturing and Automation, Published by DAAAM International, ISBN 978-3-902734-36-5, ISSN 1726-9679, Vienna, Austria, DOI: 10.2507/33rd.daaam.proceedings.022

[8] Moric, Z.; Redzepagic, J. & Gatti, F. (2021). Enterprise Tools for Data Forensics. Annals of DAAAM & Proceedings, 10(2), Published by DAAAM International, ISBN 978-3-902734-33-4, ISSN 1726-9679, Vienna, Austria, DOI: 10.2507/32nd.daaam.proceedings.014

[9] Parn, E.A. & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence, Engineering, Construction and Architectural Management, Vol. 26 No. 2, pp. 245-266., DOI: https://doi.org/10.1108/ECAM-03-2018-0101

[10] Ghafir, I.; Prenosil, V.; Svoboda, J.; & Hammoudeh, M. (2016). A survey on network security monitoring systems. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 77-82). IEEE.

[11] Ndatinya, V.; Xiao, Z.; Manepalli, V. R.; Meng, K. & Xiao, Y. (2015). Network forensics analysis using Wireshark. International Journal of Security and Networks, 10(2), 91-106.

[12] Demchenko Y.; Turkmen F.; Slawik M. & Laat C.D. (2017). Defining Intercloud Security Framework and Architecture Components for Multi-cloud Data Intensive Applications, 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 2017, pp. 945-952, DOI: 10.1109/CCGRID.2017.144.