INCIDENT DETECTION ON ENDPOINTS AND RESPONSE OPTIONS

Matej PRDA – Peter TANUŠKA – Jana URAMOVÁ

University of Žilina, Faculty of Management Science and Informatics, Slovak Republic

e-mail: prda@stud.uniza.sk, tanuska@stud.uniza.sk, jana.uramova@fri.uniza.sk

Abstract

This article presents the results of a two-phase project focused on building a centralized system for monitoring end devices and detecting security incidents in school and university environments. The main tool used was Wazuh, an open-source platform integrating EDR and SIEM functions, supplemented by MITRE ATT&CK support and agent monitoring. The project included updating the existing infrastructure, optimizing remote access, implementing a WireGuard VPN tunnel, and comparing Wazuh with OpenEDR and Greenbone tools. The results confirm that appropriately deployed open-source technologies can provide effective and scalable endpoint protection in academic networks.

Keywords**:** *Wazuh, Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), Cybersecurity, endpoint detection, MITRE ATT&CK, WireGuard, VPN, incident and vulnerability detection, agent-based monitoring, open-source*

1 INTRODUCTION

Endpoint devices—computers, laptops, servers, mobile devices, and virtual machines—are now the most common targets of cyberattacks. They are the places where attackers try to gain initial access, escalate privileges, perform malicious operations, or spread further across the network. For this reason, endpoint security is an essential element of any modern cyber infrastructure, especially in academic environments where a large number of users work and devices are exposed to a variety of risks.

The Wazuh tool was used for this purpose within the project, which is a comprehensive open-source security platform combining EDR (Endpoint Detection and Response) and SIEM (Security Information and Event Management) functions. Wazuh allows you to monitor the status of end devices, analyze system and application logs, detect suspicious behavior, search for vulnerabilities, monitor file integrity, and automatically respond to incidents. It works on the basis of agents installed on individual

devices, which collect detailed data and send it to a central server, where it is analyzed and evaluated.

Wazuh is also a very flexible tool – it can be integrated with Elastic Stack, Suricata, and services such as VirusTotal. This allows it to provide not only an overview of what is happening at the endpoint level, but also a broader context of potential attacks. [1], [2], [3], [4]

In this project, we built on previous projects and focused on the deployment, configuration, testing, and comparison of security technologies in a primary school environment and university infrastructure. The goal was to create a centralized monitoring environment, increase the security level of end devices, and verify the capabilities of modern open-source tools designed to detect and respond to security incidents.

2 METHODOLOGY AND RESULTS

Work on the project was divided into two consecutive stages carried out in 2024 and 2025, which together created a comprehensive process for building a centralized security solution for monitoring end devices. The goal was to create a system capable of unified data collection, event correlation, threat detection, and automated response in both school and university environments.

The first stage involved stabilizing the existing Wazuh deployment in the elementary school environment. Outdated components that were two major versions behind the current release were updated, which posed a risk of missing security patches and limited compatibility. Full system backups were performed, followed by server and agent upgrades and functionality testing after the update. Since the agents only worked when the school computers were turned on, they were updated during IT classes. At the same time, remote access was redesigned: the original and inefficient model via the teacher's computer was replaced by a direct XRDP connection to the server, which significantly simplified system administration and eliminated dependence on a single device. As part of this stage, a new Wazuh server was also prepared at KIS, which would later serve as a central monitoring node for the entire solution.

The second phase of the project focused primarily on integrating both environments and expanding security mechanisms. A key step was the deployment of a WireGuard VPN tunnel, which ensured secure and stable data transfer from the elementary school to the university server. After redirecting the logs to KIS, a centralized monitoring environment was created, to which agents deployed on other virtual machines and servers (XenOrchestra, ELK, Moloch, Suricata) were added. This step connected school and academic facilities into one large EDR/SIEM ecosystem. This stage also included a systematic comparison of Wazuh with the OpenEDR and Greenbone tools. OpenEDR is a pure endpoint solution capable of analyzing processes, memory, system calls, and registries in real time, but without a centralized SIEM context. Greenbone, on the other hand, focuses on network vulnerability scanning using an NVT test database and provides high-quality reports, but without an agent, it cannot detect all changes and

weaknesses directly in the operating system. The tests clearly showed that Wazuh, as an agent-based solution, identified more vulnerabilities than Greenbone thanks to its access to system layers. OpenEDR had the advantage of in-depth analysis of specific endpoint processes, but it lacked the multi-endpoint event correlation that Wazuh provides thanks to its SIEM capabilities.

An important part of the work was testing Wazuh's active response, which is a key aspect of automation. The test was performed by simulating a brute force attack on SSH on a server where the Wazuh agent was installed. The attack consisted of generating repeated unsuccessful login attempts from a defined IP address. Thanks to its rules, Wazuh detected an excessive number of attempts, evaluated the incident, and automatically triggered an active response action—specifically, temporarily blocking the attacker's IP address on the firewall. After a predefined time interval, the system automatically unblocked the attacker, confirming the correct functioning of the entire mechanism. This test demonstrated Wazuh's practical ability to respond to incidents without administrator intervention, thereby increasing the level of protection for critical systems.

The second stage also included testing notification delivery options. Three solutions currently most commonly used by operational security teams were evaluated: Microsoft Teams, Slack, and PagerDuty. Integration with Microsoft Teams was complicated due to a change in the functioning of webhooks, which were no longer compatible with the way Wazuh generates notifications. Slack offered a simple connection in older versions, but its current free version no longer supports webhooks, which made testing impossible. Finally, sending notifications via PagerDuty was successfully configured and tested, providing reliable alerting with the option of subsequent incident escalation, although it is a commercial service. Testing all three options identified the technical limitations of free platforms and confirmed that Wazuh can work effectively with professional notification tools.

The result of all these steps was the transformation of the original solution into a fully centralized and scalable security system capable of monitoring endpoints in two different types of infrastructure, analyzing threats in real time, and automating incident response. The resulting system provides a robust foundation for further development and long-term improvement of cybersecurity.

3 CONCLUSION

The project succeeded in building a functional and centralized system for monitoring end devices and detecting incidents in school and university environments. Updates and enhancements to the Wazuh tool have resulted in more stable data collection, more advanced analysis capabilities, and more reliable threat identification. The implementation of a VPN tunnel has achieved a secure connection between both environments, making it possible to process all events on a single central server. A comparison of Wazuh with the OpenEDR and Greenbone tools revealed differences between these tools. The project confirmed that modern open-source solutions can

provide effective infrastructure protection even in environments with diverse requirements. The created system is ready for further expansion and provides a solid foundation for long-term improvement of cybersecurity.

Acknowledgement: Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I05-03-V02-00010.

REFERENCES

[1] “Wazuh - Open Source XDR. Open Source SIEM.” Accessed: Nov. 25, 2025. [Online]. Available: https://wazuh.com/

[2] “Wazuh documentation.” Accessed: Nov. 25, 2025. [Online]. Available: https://documentation.wazuh.com/current/index.html

[3] N. AKSHAI SANKAR and K. A. FASILA, "Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring," 2023 9th International Conference on Smart Computing and Communications (ICSCC), Kochi, Kerala, India, 2023, pp. 350-354, doi: 10.1109/ICSCC59169.2023.10334992.

[4] S. MOIZ, A. MAJID, A. BASIT, M. EBRAHIM, A. A. ABRO and M. NAEEM, "Security and Threat Detection through Cloud-Based Wazuh Deployment," 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), Tandojam, Pakistan, 2024, pp. 1-5, doi: 10.1109/KHI-HTC60760.2024.10482206.