JCSAS
Journal of Community Service and Application of Science
ISSN:2962 - 2263, Vol.05, No.01, June, 2026, hal. 9- 16

Strengthening Cybersecurity Capacity Through the Implementation of Wazuh on the Server Infrastructure of LLDIKTI Region X

Karfindo[1]*, Hasan[2], Muhammad Diponegoro[3], Yusril Eka Mahendra[4], Mohammad Arifin[5]
[1]Pontianak State Polytechnic
Email:[1]karfindo@polnep.ac.id, [2]indra_elka@yahoo.co.id, [3]muhammaddiponegoro@gmail.com, [4]yusrilekamahendra@polnep.ac.id, [5]mohamad.arifin@polnep.ac.id
*Corresponding author: Karfindo (karfindo@polnep.ac.id)

Article History:
Received:01-08-2026
Revised:04-08-2026
Accepted:05-08-2026
Published:05-08-2026

Abstract
Higher education service institutions increasingly depend on digital infrastructure, yet security monitoring of their servers is frequently absent, so incidents remain undetected until reported by outside parties. This community service programme addressed that gap at Lembaga Layanan Pendidikan Tinggi (LLDIKTI) Region X, whose service applications run on Proxmox hypervisors hosting Ubuntu virtual machines without any centralised security monitoring. The objectives were to raise the technical understanding of the institution's IT personnel and to bring a working security monitoring system into operation on the partner's infrastructure. The programme combined technology diffusion, demonstration of technology, and mentoring. It was delivered at the STTIND Padang campus to fifteen IT managers attending on site, with the resource person presenting remotely by video conference, and continued afterwards as mentoring while the partner's own team carried out the installation. Nine structured modules covered the threat landscape, Wazuh architecture, agent deployment, log and alert analysis, file integrity monitoring, active response, vulnerability detection and security configuration assessment, an integrated attack scenario, and a thirty-day operational roadmap. Wazuh now operates on the partner's infrastructure in an all-in-one configuration with centralised log analysis, file integrity monitoring, vulnerability detection, configuration assessment, and automated response. The institution has moved from a reactive to a proactive security posture, sustained by a fifteen-minute daily operational checklist that the partner has adopted.
Keywords: *community service; file integrity monitoring; open source; security monitoring; Wazuh*

INTRODUCTION

The Higher Education Service Institute (LLDIKTI) Region X provides services to private universities in West Sumatra, Riau, Jambi, and the Riau Islands. Nearly all of these services, from managing educator and staff data, proposing academic positions, to disseminating public information, are now delivered through a web-based application. This reliance places server availability and integrity as prerequisites for service quality: when a server goes down, services to hundreds of private universities are disrupted.

A situational analysis of the partner's infrastructure revealed that the service was supported by a number of servers with a Proxmox hypervisor running Ubuntu Server virtual machines with a web management panel. While the infrastructure functioned well, it lacked a centralized security monitoring system. The consequences were fundamental: administrators lacked visibility into who was accessing the servers, what files were changing, and whether any anomalous activity was occurring. Incident management was also reactive, meaning issues were only discovered after user complaints or third-party reports.

This situation is not unique to one institution. The National Cyber and Crypto Agency recorded more than 403 million traffic anomalies in Indonesia throughout 2023, with the education sector among the most vulnerable targets (1). Educational institution domains are often misused to insert online gambling content due to their high search engine reputation. Other common attack patterns targeting institutional servers include illegal crypto mining, recruiting servers into bot networks, and data theft and hostage taking. The problem is further exacerbated by the long time between intrusion and detection of an incident globally, averaging 194 days for identification and 64 days for recovery (2). This means attackers can remain in a system for months without detection.

JCSAS
Journal of Community Service and Application of Science
ISSN:2962 - 2263, Vol.05, No.01, June, 2026, hal. 9- 16

From a regulatory perspective, Law Number 27 of 2022 concerning Personal Data Protection places electronic system administrators as data controllers, obligated to maintain the confidentiality of personal data and notify data subjects of any leaks within 3x24 hours (3). This obligation is practically impossible to fulfill without a monitoring system that records an audit trail, as institutions cannot report undetected leaks and cannot prove compliance without forensic evidence.

A technical solution to this problem is readily available in the form of a Security Information and Event Management (SIEM) platform. However, commercial SIEM solutions generally employ a data-volume-based licensing model that is difficult for educational institutions to afford. Wazuh, on the other hand, provides equivalent capabilities, combining SIEM, Extended Detection and Response (XDR), and Host-based Intrusion Detection System (HIDS) as open-source software that can be fully deployed internally without relying on third-party cloud services (4). Several studies in Indonesia have demonstrated Wazuh's effectiveness for server security monitoring in various organizational contexts, both for log aggregation and detection of forced login attempts (5) and for file integrity monitoring and website threat tracking (6), providing sufficient empirical basis for this technology choice.

However, the availability of free software does not automatically guarantee security. The main obstacle lies in human resource capacity. Information technology managers need to understand system architecture, be able to install and configure it, read and interpret alerts, and most importantly, consistently implement operational routines. Therefore, the intervention chosen in this community service program does not stop at delivering materials but continues as mentoring until the system is fully installed and operational on the partner's infrastructure by the partner's own team.

Based on the description, the objectives of this community service activity are: (1) to increase the understanding of LLDIKTI Region X information technology managers regarding the cyber threat landscape on institutional servers and the urgency of security monitoring; (2) to introduce the workings, architecture, and operating procedures of the Wazuh platform; (3) to accompany partners until the Wazuh-based security monitoring system operates on their server infrastructure; and (4) to prepare operational guidelines and a follow-up roadmap so that its implementation is sustainable after the activity ends.

METHOD

Venues and Activity Partners

The activity was carried out as part of the IT, Application, and Server Management Human Resource Competency Improvement program organized by LLDIKTI Region X, located at the Padang Industrial Technology College (STTIND) Campus. The activity partner is LLDIKTI Region X, specifically the Information Systems and Cooperation Working Group Team (Pokja SIK) as the institution's information technology infrastructure management unit. The participants numbered fifteen people consisting of application, network, and server managers within the LLDIKTI Region X environment. This article specifically reports on the Server Security Monitoring session with Wazuh along with assistance in its implementation.

Mode of Implementation

The event was held in a blended format. Participants participated offline in the training room at the STTIND Padang Campus, while resource persons delivered and demonstrated the material online via video conference, broadcast on the room's main screen. This mode was chosen for efficiency and to take advantage of the material's entirely command-line and browser-based nature, allowing for a fully readable demonstration through screen sharing.

Subject Characteristics and Involvement

Participants were technical personnel accustomed to managing servers and production applications, but had no experience operating a centralized security monitoring platform. This characteristic determined the activity's design: the material was not designed as an introduction to information security for beginners, but rather as a transfer of operational knowledge for practitioners. Partner involvement was active from the planning stage. Infrastructure needs and conditions were identified with the SIK Working Group Team before the material was developed, so all examples, topologies, and scenarios demonstrated were based on the partner's actual infrastructure, not a generic environment. During the implementation phase, the partner team itself executed the installation and configuration, while the resource person acted as a mentor.

Implementation Method

The activity uses a combination of three complementary community service methods. First, science and technology diffusion, in the form of an introduction to security monitoring concepts and technologies that are not yet used by partners, including the threat landscape, the confidentiality-integrity-availability triad, the principle of layered defense, and the cyber attack chain model (7) mapped against publicly documented attacker tactics and

JCSAS
Journal of Community Service and Application of Science
ISSN:2962 - 2263, Vol.05, No.01, June, 2026, hal. 9- 16

techniques (8). Second, science and technology simulation, in the form of a live demonstration of each procedure by a resource person through screen sharing, starting from installing the Wazuh Server, registering agents, reading alerts, to configuring automatic responses, so that participants get a concrete picture of how the system works before implementing it themselves. Third, advocacy and mentoring, in the form of mentoring the partner team during implementation in the institution's infrastructure, accompanied by the submission of operational guidelines and a follow-up roadmap.

Activity Stages

Implementation is divided into four stages as presented in Table 1.

Table 1. Stages of Community Service Activity Implementation

Level	Activity	Exterior
I. Preparation	Coordination with the SIK Working Group Team, identification of infrastructure conditions and partner needs, preparation of nine handout modules, preparation of video conference channels	Training modules and implementation architecture design
II. Delivery of material	Presentation and demonstration of nine modules online to participants who attended offline, accompanied by a question and answer session and case discussion.	Participants understand the architecture, procedures, and operating methods of Wazuh.
III. Implementation	Installation of Wazuh Server on a dedicated virtual machine and agent registration on the target server, carried out by the partner team with assistance from resource persons	Monitoring system is in operational status
IV. Follow-up assistance	Preparation of daily, weekly and monthly operational checklists, preparation of 30-day roadmaps, and remote technical consultations	Operational guidelines and sustainability commitments

Material Presented

The material is structured into nine modules with a flow from conceptual understanding to operational capabilities, as presented in Table 2. This tiered arrangement is intended so that participants do not simply copy technical commands, but rather understand the reasons behind each configuration.

Table 2. Structure of Server Security Monitoring Material with Wazuh

Module	Topic	Expected achievements
1	Why do servers need to be monitored?	Understanding the threat landscape, attack motives, and incident impact
2	Wazuh architecture and implementation design	Understand the roles of the Manager, Indexer, Dashboard, and Agent components and design an all-in-one implementation.
3	Agent implementation	Understand the procedures for installing, registering, and verifying agent data flows.
4	Logs and alerts	Understanding the event-alert-incident hierarchy, severity levels 1-15, and alert anatomy
5	File integrity monitoring	Understanding web directory monitoring configuration and how to investigate file changes
6	Automatic response	Understanding automatic blocking configuration and the importance of whitelisting
7	Vulnerability detection and security configuration assessment	Read vulnerability scan results and configuration assessment scores and prioritize remediation
8	Integrated scenario	Understand the stages of a real attack and the detection points at each stage.
9	Daily operations and 30-day roadmap	Establish operational routines, alert setup, backup procedures, and follow-up plans.

Success Indicators

Because the primary output of this activity is an operational system, success is not measured through written tests but rather through proof of functionality and sustainability for partners. Indicators used include: (a) the three core Wazuh services running on the partner's infrastructure: Manager, Indexer, and Dashboard; (b) the agent connecting to the target server so that data flows to the dashboard; (c) the file integrity monitoring,

JCSAS
Journal of Community Service and Application of Science
ISSN:2962 - 2263, Vol.05, No.01, June, 2026, hal. 9- 16

vulnerability detection, security configuration assessment, and automated response modules being active; (d) the partner team's ability to carry out installation and configuration themselves with assistance; and (e) the development and agreement of operational routines and a follow-up roadmap.

RESULTS AND DISCUSSION

Initial Conditions of Partners

Identification during the preparation phase revealed that the partner's infrastructure was well-organized in terms of virtualization and application management, but a security monitoring layer was missing. Log files were stored separately on each virtual machine, not aggregated, and practically never reviewed. There was no mechanism to notify managers when files in the service directory changed, when a forced login attempt occurred, or when installed software contained a published vulnerability. A summary of the pre- and post-implementation conditions is presented in Table 3.

Table 3. Comparison of Partner Server Security Management Conditions Before and After the Activity

Aspect	Before	After
Log aggregation	Separate per machine and not reviewed	Centered on Wazuh Indexer and searchable
Incident detection	After there is a complaint or report from an external party	Near real-time automatic alerts
Service file integrity	Not monitored	Monitored via the file integrity monitoring module
Response to attacks	Manual and subject to personnel availability	Auto response with whitelist
Vulnerability management	Patching is incidental	Based on the list of findings sorted by severity
Forensic evidence	Not available	Event timeline is saved and can be reconstructed
Operational routines	There isn't any yet	Daily, weekly, and monthly checklists

Implementation of Activities

The training consisted of brief conceptual presentations followed by live demonstrations for each module. The resource person displayed the terminal, configuration files, and Wazuh dashboard via screen sharing, while participants observed and asked questions at each stage. The training room environment is shown in Figure 1, while the resource person's online presentation via video conference is shown in Figure 2

.

Figure 1. The atmosphere of the implementation of activities at the STTIND Padang Campus

JCSAS
Journal of Community Service and Application of Science
ISSN:2962 - 2263, Vol.05, No.01, June, 2026, hal. 9- 16

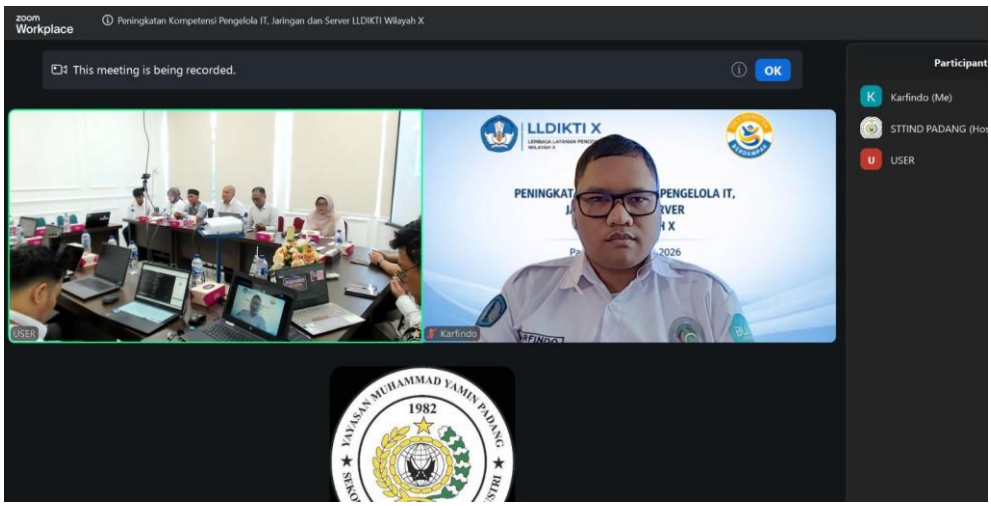

Figure 2. Presentation of material by resource persons online to participants attending offline

The case-based approach in the opening module proved effective in building urgency. Rather than starting with technical definitions, the module opened with a scenario involving the insertion of gambling content on an institutional website—a scenario familiar to participants due to its frequent occurrence in the educational domain. The reflective discussion that followed fostered a shared awareness that lack of visibility is a risk that has been tacitly accepted. The Q&A sessions in subsequent modules were filled with contextual questions about the condition of the servers they manage, demonstrating the relevance of the material to the participants' real-life problems.

System Implementation on Partner Infrastructure

After completing the series of materials, the SIK Working Group (Pokja SIK) independently installed Wazuh on the institution's infrastructure, assisted by a resource person. The all-in-one deployment model was chosen because it places Wazuh Manager, Indexer, and Dashboard on a single dedicated virtual machine, simplifying installation and maintenance while providing sufficient capacity for small to medium-sized environments. The virtual machine was placed separately from the machines running production services, as the Indexer component requires significant memory allocation and could potentially disrupt the performance of other services when combined. The implemented configuration is summarized in Table 4.

Table 4. Wazuh Deployment Configuration on Partner Infrastructure

Aspect	Applied configuration
Implementation model	All-in-one, namely Manager, Indexer, and Dashboard on one virtual machine
Placement	Dedicated virtual machine, separate from production service virtual machines
Operating system	Linux distribution with long-term support
Monitoring coverage	Servers and service virtual machines in partner environments
Activated modules	Log analysis, file integrity monitoring, vulnerability detection, security configuration assessment, and automated response
Communication channels	Internal agency network, with agent to Manager traffic encrypted
Dashboard access	Limited to internal network via browser
Final status	All three core services are running and the agent is sending data to the dashboard.

The decision to have the partner team execute the installation was a conscious one. While having a resource person handle the work, the system would have been up and running more quickly, but operational knowledge wouldn't have transferred, and the partner would have been dependent on an external party for any configuration changes. By having a resource person as a companion, challenges that arose during the installation, such as adjusting traffic filtering rules between machines to allow agents to reach the Manager, became learning experiences that stuck with the partner team.

Introduced Detection Capabilities and Limits

A key component of the material is mapping Wazuh's detection capabilities to the stages of a real-world attack. Through integrated scenario modules, participants are introduced to the attack flow, from reconnaissance,

JCSAS
Journal of Community Service and Application of Science
ISSN:2962 - 2263, Vol.05, No.01, June, 2026, hal. 9- 16

initial access through forced entry, backdoor installation, system exploration, and service file modification, along with the Wazuh modules involved in each stage. Log analysis plays a role in initial access and scheduled task changes, file integrity monitoring plays a role in backdoor installation and service page modification, and automated responses play a role in shutting down attacker access without requiring human intervention.

The material also openly communicates the platform's limitations, as understanding limitations is just as important as understanding capabilities. Port scanning at the network layer leaves no trace in operating system logs and is therefore undetectable without integration with a network intrusion detection system. Deleting command history requires enabling command-level auditing. Data leaving the system is beyond the reach of the platform, as Wazuh is not a data breach prevention tool. Communicating these limitations is crucial to prevent partners from developing a false sense of security after installing a single tool, and serves as the basis for recommendations for layered reinforcements in subsequent phases.

Vulnerability detection and security configuration assessment modules were introduced as prioritization tools. Both produce a list of findings ranked by severity and a list of configuration items that do not conform to widely referenced best practices (9). The advantage of this approach for partners is that it provides objective prioritization: patches are no longer based on guesswork but rather on risk levels, allowing limited technical resources to be directed to the greatest risks first.

Governance Change and Sustainability

The most crucial achievement for sustainability is not the establishment of software, but rather the establishment of routines. The final module establishes realistic operational routines: a fifteen-minute daily review that includes checking high-severity alerts, agent status, storage space, and automated response logs; a thirty-minute weekly review for vulnerability findings, configuration assessment scores, and rule updates; and a monthly review for whitelist updates, configuration backups, and reporting to leadership. These regular routines align with the principle of continuous security monitoring, which views monitoring as a process, not a single event (10).

The routine is accompanied by a thirty-day roadmap that divides follow-up into four weekly phases: strengthening the foundation on the most critical machines, expanding agent coverage to all servers, optimizing through rule tuning and vulnerability remediation, and maturing through application log integration, notification setup, and knowledge transfer to teammates. The last point is emphasized to avoid relying on a single person to operate the system, a common organizational risk in small IT units.

Alert tuning is a special focus because it's the most common cause of SIEM implementation failure. Systems that generate hundreds of alerts daily, most of which aren't real threats, will eventually be ignored by their operators, resulting in the truly important ones being missed. Participants were therefore equipped with techniques to create custom rules to scale up or down based on the partner's environment, along with reasonable alert volume targets after several weeks of tuning.

Discussion

The success of this activity rests on three factors. First, the technology's suitability to the partner's specific needs. Wazuh can be fully installed on internal infrastructure without licensing fees and without reliance on cloud services, thus meeting both budget constraints and the data sovereignty needs of government agencies. Second, the use of real-world partner contexts throughout the material. The topologies, directory paths, and management panels used in the demonstrations are those actually used by partners, significantly shortening the gap between the training room and the production environment. Third, the continuation of the activity through to the implementation stage distinguishes this service from activities that stop at the delivery of the material.

A mentoring approach that places the partner team in charge of the installation process yields qualitatively different results compared to delivering a finished system. A similar experience was reported in the development of a Wazuh-based server security monitoring system in a university environment, which concluded that improving administrators' ability to respond to incidents was as important an achievement as establishing the system itself (11). An additional contribution of this service lies in emphasizing that successful implementation is not determined solely by the technical capabilities of the device, but rather by the development of operational capacity and routines within the partner organization.

The blended learning model also provided unique lessons. Online delivery proved adequate for command-line-based technical materials, as all learning objects, including terminals, configuration files, and dashboard interfaces, could be displayed via screen sharing with improved readability compared to conventional projections. The presence of offline participants in the same room remained crucial, maintaining the pace of the activity and enabling participants to engage in discussions with one another. A perceived limitation was the reduced ability of the resource person to monitor each participant's understanding at a glance. This was addressed through structured Q&A sessions at the end of each module and the provision of complete written modules containing commands,

JCSAS
Journal of Community Service and Application of Science
ISSN:2962 - 2263, Vol.05, No.01, June, 2026, hal. 9- 16

prerequisite lists, verification checklists, and problem-tracking tables for independent review. This configuration also reduced implementation costs and made the activity model easier to replicate for other institutions in the same region.

Challenges encountered during implementation included limited time to explore all platform capabilities in depth, varying levels of experience among participants, which resulted in uneven learning speeds, and the Indexer component's substantial memory requirements, necessitating the allocation of a dedicated virtual machine. These challenges were addressed through the provision of self-paced written modules, follow-up consultation sessions after the event, and agreed-upon capacity planning with partners prior to implementation.

CONCLUSION

This community service activity increased the cybersecurity capacity of LLDIKTI Region X through an approach that combined material delivery, technology demonstrations, and implementation assistance. Partner information technology managers gained an understanding of the threat landscape to institutional servers, the architecture and operation of the Wazuh platform, and its operational procedures. Furthermore, a security monitoring system is now operational on the partner's infrastructure and was installed by the partner's own team with assistance, including centralized log analysis, file integrity monitoring, vulnerability detection, security configuration assessment, and automated response. The most valuable change was the shift in security management from a reactive to a proactive approach, supported by daily operational routines and a follow-up roadmap agreed upon with the partner. The mixed-mode implementation also demonstrated that technical knowledge transfer can be effective even though the resource person delivered the material remotely.

Further community service activities are recommended to expand the scope to private universities in the LLDIKTI Region X environment that face similar problems with generally more limited resources, complement the implementation with the integration of network-level intrusion detection systems and command-level audits to close the identified detection gaps, and conduct periodic mentoring accompanied by measurements to assess operational maturity in the medium term.

THANK-YOU NOTE

The author would like to thank the Higher Education Service Institution of Region X for their trust and support in organizing the activity, especially to the Head of LLDIKTI Region X, Dr. Afdalisma, S.H., M.Pd., and the Information Systems and Cooperation Working Group Team for their active involvement from the planning stage to implementation. Thanks are also extended to the Padang Industrial Technology College (STTIND) and its Chairperson, Riko Ervil, S.T., M.T., IPU, for providing facilities for organizing the activity, as well as to all participants for their active participation during the activity.

BIBLIOGRAPHY

1. National Cyber and Crypto Agency. Indonesian Cybersecurity Landscape 2023 [Internet]. 2024 [accessed August 1, 2026]. Link: https://www.bssn.go.id/
2. IBM Security. Cost of a Data Breach Report 2024 [Internet]. 2024 [accessed August 1, 2026]. Link: https://www.ibm.com/reports/data-breach
3. Government of the Republic of Indonesia. Law Number 27 of 2022 concerning Personal Data Protection; 2022.
4. Wazuh Inc. Wazuh Documentation: The Open Source Security Platform [Internet]. 2024 [accessed August 1, 2026]. Link: https://documentation.wazuh.com/current/
5. Aditya R, Muhyidin Y, Singasatia D. Implementation of Security Information and Event Management (SIEM) for Server Security Monitoring Using Wazuh. Mercury: Journal of Information Systems and Informatics Engineering Research. 2024; 2(5): 137-144.
6. Hidayasari N, Mansur, Kasmawi, Efendi Z. Implementation of Wazuh-Based SIEM Prototype on Website with FIM Testing and Threat Hunting. JITSI: Scientific Journal of Information Systems Technology. 2025; 6(4): 372-382.
7. Hutchins EM, Cloppert MJ, Amin RM. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Leading Issues in Information Warfare & Security Research. 2011; 1(1): 80-106.
8. MITRE Corporation. MITRE ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge [Internet]. 2024 [accessed August 1, 2026]. Link: https://attack.mitre.org/

JCSAS
Journal of Community Service and Application of Science
ISSN:2962 - 2263, Vol.05, No.01, June, 2026, hal. 9- 16

9. Center for Internet Security. CIS Benchmarks [Internet]. 2024 [accessed August 1, 2026]. Link: https://www.cisecurity.org/cis-benchmarks
10. National Institute of Standards and Technology. NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Gaithersburg: National Institute of Standards and Technology; 2011.
11. Wahid A, Agung M, Parenreng JM, Sunusi SL. PKM Development of Security Monitoring System for SIMLP2M UNM Application Server Using Wazuh [Internet]. 2024 [accessed on August 1, 2026]. Link: https://ict.unm.ac.id/2024/09/05/pkm-pengembangan-sistem-monitoring-keamanan-server-aplikasi-simlp2m-unm-gunakan-wazuh/