Implementasi Firewall Untuk Keamanan Dan Pencegahan Serangan Siber Di SMAI Kepanjen Kabupaten Malang

Yuri Ariyanto[1*)], Yan Watequlis Syaifudin[2)]. Budi Harijanto[3)], Chandrasena Setiadi[4)], M Hasyim Ratsanjani[5)], Hendra Pradibta[6)], Ali Ridho Muladawila[7)], Didik Sunariyanto[8)]

[1]Jurusan Teknologi Informasi, Politeknik Negeri Malang
email: yuri@polinema.ac.id
[2]Jurusan Teknologi Informasi, Politeknik Negeri Malang
email: qulis@polinema.ac.id
[3]Jurusan Teknologi Informasi, Politeknik Negeri Malang
email: budi.harijanto@polinema.ac.id
[4]Jurusan Teknik Elektro, Politeknik Negeri Malang
email: chandrasenasetiadi@polinema.ac.id
[5]Jurusan Teknologi Informasi, Politeknik Negeri Malang
email: hsy@polinema.ac.id
[6]Jurusan Teknologi Informasi, Politeknik Negeri Malang
email: hendra.pradibta@polinema.ac.id
[7]Jurusan Teknologi Informasi, Politeknik Negeri Malang
email: aliridhomuladawila@gmail.com
[8]SMA Islam Kepanjen, Kabupaten Malang
email: masdiksun@gmail.com

Abstract

The implementation of a firewall-based network security system has become increasingly important in maintaining data integrity and availability within educational institutions. The Community Service Program (PPM) conducted by Politeknik Negeri Malang aims to enhance the network security infrastructure at SMA Islam Kepanjen, Malang Regency, through the implementation of Wazuh as a cybersecurity solution. This approach includes the installation and configuration of network infrastructure, security audits, and training for IT staff on independent firewall management. The implementation methodology involves site surveys, network topology design, hardware and software installation, system testing, and technical mentoring. The outcomes achieved include increased awareness of cybersecurity issues and improved capacity of partner personnel in managing the network infrastructure. With the implementation of Wazuh, it is expected that SMA Islam Kepanjen will be able to proactively address cyber threats and serve as a model for information technology implementation in other schools across Malang Regency.

Keywords: Wazuh, Network Security, Community Service Program, Cyber Threat, Network Infrastructure

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mengubah pola interaksi serta pengelolaan data di berbagai sektor, termasuk dalam dunia pendidikan. Sekolah sebagai institusi pendidikan tidak hanya menjadi tempat proses belajar-mengajar, tetapi juga pusat pengelolaan data penting seperti biodata siswa, hasil ujian, hingga sistem administrasi kependidikan. Dalam konteks ini, jaringan komputer memegang peran vital dalam mendukung efisiensi dan efektivitas operasional sekolah. Namun, peningkatan ketergantungan pada sistem digital juga membawa risiko keamanan siber yang semakin kompleks. Ancaman seperti *malware, phishing*, intrusi jaringan, hingga pencurian data dapat terjadi kapan saja, terutama pada institusi dengan infrastruktur keamanan yang belum memadai (Malik et al., 2022).

SMA Islam Kepanjen, Kabupaten Malang, merupakan salah satu institusi pendidikan menengah yang sedang berupaya meningkatkan kualitas layanan pendidikannya melalui pemanfaatan teknologi informasi. Berdasarkan hasil observasi awal

permasalahan yang dihadapi oleh SMA Islam Kepanjen pada jaringan komputer yang digunakan masih rentan terhadap ancaman siber eksternal akibat kurangnya kontrol akses dan minimnya sistem proteksi yang memadai. Selain itu, staf IT yang bertugas belum memiliki kapasitas penuh dalam mengelola keamanan jaringan secara mandiri. Infrastruktur jaringan yang ada tidak dirancang untuk menangkal ancaman modern, sehingga rawan terhadap potensi pelanggaran keamanan yang dapat mengganggu kelancaran aktivitas belajar mengajar serta merusak reputasi institusi (Pujiantoro & Nugraha, 2025).

Mengingat urgensi perlindungan data dan keberlanjutan operasional institusi pendidikan, diperlukan solusi konkret yang mampu meningkatkan ketahanan jaringan komputer. Salah satu strategi yang efektif adalah implementasi *firewall* berbasis open source seperti *Wazuh (Amami et al., 2024; Moiz et al., 2024)*, yang tidak hanya memberikan perlindungan terhadap serangan eksternal, tetapi juga menyediakan fitur deteksi intrusi dan manajemen keamanan secara terpusat. Pendekatan ini sejalan dengan rekomendasi beberapa studi yang menyebut bahwa penggunaan *firewall* generasi baru sangat efektif dalam meningkatkan pertahanan siber (N. Sun et al., 2023; P. J. Sun, 2020). Selain itu, penerapan sistem keamanan berbasis perangkat lunak open source dinilai lebih ekonomis dan fleksibel dibandingkan solusi proprietary, terutama untuk institusi dengan anggaran terbatas seperti sekolah swasta (Ariyanto et al., 2025; Bhasin et al., 2020).

Program Pengabdian kepada Masyarakat (PPM) yang dilaksanakan oleh Politeknik Negeri Malang bertujuan untuk menjawab tantangan tersebut melalui implementasi *firewall* menggunakan *Wazuh* sebagai solusi keamanan jaringan di SMA Islam Kepanjen. Kegiatan ini mencakup survei lokasi, desain topologi jaringan, instalasi perangkat keras dan lunak, audit keamanan, serta pelatihan dan pendampingan teknis bagi staf IT. Tujuan utamanya adalah meningkatkan kapasitas internal mitra dalam mengelola jaringan secara aman dan mandiri, sekaligus membangun pondasi keamanan jaringan yang kuat guna mendukung kelancaran kegiatan pendidikan dan administrasi.

Selain itu, program ini juga memiliki dimensi edukatif yang penting. Melalui pelatihan dan seminar, guru dan staf IT akan memperoleh pemahaman tentang praktik keamanan siber terkini, termasuk cara mendeteksi ancaman, melakukan respons insiden, serta menerapkan kebijakan keamanan jaringan yang sesuai standar. Hal ini selaras dengan temuan (N. Sun et al., 2023), yang menunjukkan bahwa penguasaan konsep dasar jaringan dan keamanan siber sangat berpengaruh terhadap kemampuan pengelolaan sistem oleh tenaga teknis di institusi pendidikan. Dengan demikian, PPM ini tidak hanya memberikan manfaat langsung berupa infrastruktur yang lebih aman, tetapi juga menciptakan dampak berkelanjutan melalui peningkatan kapasitas sumber daya manusia (Ariyanto, 2023).

Secara lebih luas, keberhasilan implementasi sistem keamanan jaringan di SMA Islam Kepanjen diharapkan dapat menjadi model bagi sekolah-sekolah lain di wilayah Kabupaten Malang. Upaya ini relevan dengan visi Politeknik Negeri Malang dalam merevitalisasi infrastruktur sosial dan pendidikan melalui penerapan ilmu pengetahuan dan teknologi. Dengan adanya kolaborasi antara perguruan tinggi dan mitra sekolah, diharapkan tercipta sinergi yang bermakna dalam membangun budaya keamanan digital yang proaktif dan berkelanjutan.

2. KAJIAN LITERATUR DAN PEGEMBANGAN HIPOTESIS

Peningkatan ancaman keamanan siber di sektor pendidikan menjadi perhatian serius dalam beberapa tahun terakhir (Azzahra et al., 2024). Jaringan komputer yang digunakan oleh institusi pendidikan, termasuk sekolah menengah seperti SMA Islam Kepanjen, Kabupaten Malang, rentan terhadap berbagai jenis serangan, mulai dari pencurian data sensitif hingga gangguan operasional akibat intrusi eksternal (Ariyanto et al., 2025; Khraisat & Alazab, 2021). Penelitian yang dilakukan oleh Sun (P. J. Sun, 2020), menunjukkan bahwa lebih dari 60% institusi pendidikan di Asia Tenggara mengalami setidaknya satu insiden keamanan siber dalam dua tahun terakhir (Dumitrasc, 2023). Salah satu penyebab utama kerentanan ini adalah kurangnya implementasi sistem proteksi yang

memadai, seperti firewall dan sistem deteksi intrusi (Ariyanto, 2023).

Wazuh sebagai solusi *open source* untuk manajemen keamanan jaringan telah terbukti efektif dalam berbagai konteks organisasi, termasuk pendidikan. Menurut (Moiz et al., 2024; Stanković et al., 2022), Wazuh mampu menyediakan fitur *host-based intrusion detection system* (HIDS), pengawasan log aktivitas secara real-time, serta integrasi dengan sistem manajemen keamanan lainnya. Keunggulan *Wazuh* dibandingkan solusi perangkat lunak lainnya adalah biaya implementasi yang lebih rendah dan fleksibilitas dalam penyesuaian kebutuhan spesifik institusi (Khan et al., 2022; N. Sun et al., 2023), seperti yang diperlukan oleh SMA Islam Kepanjen.

Kajian empiris juga menunjukkan pentingnya pelatihan teknis bagi staf IT dalam rangka meningkatkan kapasitas internal institusi pendidikan.(Ariyanto et al., 2020), menjelaskan bahwa dengan melakukan implementasi secara langsung mampu meningkatkan kemampuan staf dalam mengelola firewall. Hal ini relevan dengan kondisi mitra yang memiliki keterbatasan pengetahuan teknis tentang pemeliharaan jaringan dan respons terhadap insiden keamanan.

Selain itu, survei yang dilakukan oleh (Bhasin et al., 2020), menegaskan bahwa strategi pengabdian yang melibatkan partisipasi aktif pihak mitra dalam proses implementasi teknologi memiliki dampak yang lebih berkelanjutan. Pendekatan partisipatif tersebut akan diterapkan dalam Program Pengabdian kepada Masyarakat (PPM) Politeknik Negeri Malang, yaitu melalui pendampingan teknis dan workshop praktis penggunaan *Wazuh (Ashiq et al., 2024)*.

Berdasarkan literatur dan bukti empiris tersebut, hipotesis yang diajukan dalam PPM ini adalah bahwa implementasi sistem keamanan jaringan berbasis *Wazuh*, disertai pelatihan dan pendampingan teknis, akan meningkatkan ketahanan siber SMA Islam Kepanjen secara signifikan. Selain itu, partisipasi aktif staf IT dalam proses implementasi akan meningkatkan kapasitas internal dan membantu pembentukan budaya keamanan digital yang berkelanjutan. Pada Tabel 1 ditunjukkan ringkasan tentang kajian literatur.

Tabel 1. Ringkasan Kajian Literatur Terkait PPM

No	Literatur	Relevansi
1	Amami et al. (2024)	Mendukung pemilihan Wazuh sebagai solusi keamanan
2	Sun (2020)	Memperkuat urgensi implementasi sistem keamanan
3	Hernandez et al. (2019)	Menjadi dasar teknis implementasi
4	Ariyanto et al. (2025)	Dasar metode pendampingan implementasi firewall

3. METODE

Metode pelaksanaan dalam Program Pengabdian kepada Masyarakat (PPM) dengan judul "Implementasi Firewall untuk Keamanan dan Pencegahan Serangan Siber di SMA Islam Kepanjen, Kabupaten Malang" dirancang secara sistematis untuk menjawab permasalahan yang dihadapi oleh mitra terkait kerentanan jaringan komputer, keterbatasan infrastruktur keamanan, serta kurangnya pengetahuan teknis staf IT. Pendekatan yang digunakan melibatkan beberapa tahap penting, yaitu survei lokasi, desain topologi jaringan, instalasi dan konfigurasi firewall berbasis *Wazuh*, audit keamanan, pelatihan teknis, serta pendampingan pasca-implementasi.

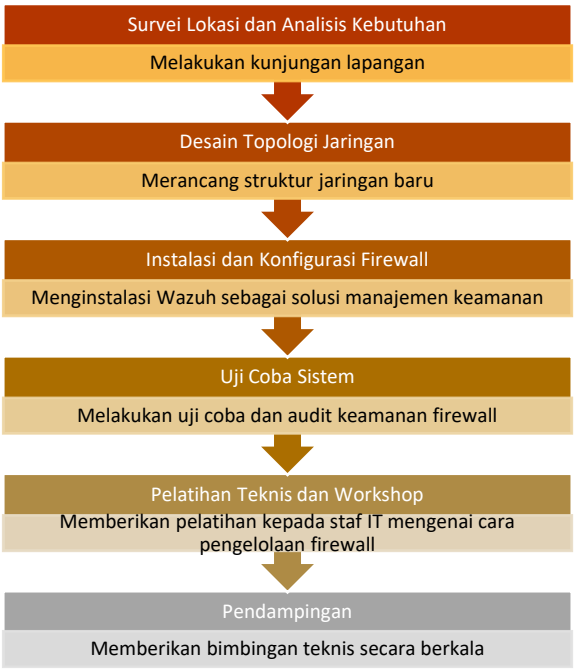
Ruang lingkup kegiatan mencakup laboratorium komputer SMA Islam Kepanjen sebagai objek utama implementasi, dengan fokus pada peningkatan keamanan jaringan internal dan perlindungan data sensitif milik siswa dan staf. Selain itu, program ini juga bertujuan meningkatkan kapasitas sumber daya manusia di bidang pengelolaan keamanan jaringan melalui pelatihan dan workshop intensif.

Bahan dan alat utama yang digunakan dalam pelaksanaan program ini meliputi server atau perangkat keras sebagai host *Wazuh*, perangkat lunak open source seperti *Wazuh Manager, Elastic Stack* untuk visualisasi log,

serta router dan switch jaringan untuk membangun arsitektur keamanan yang aman dan tersegmentasi. Selain itu, modul pembelajaran digital disusun untuk mendukung proses pelatihan dan transfer pengetahuan kepada tim IT sekolah.

Tempat pelaksanaan berada di SMA Islam Kepanjen, Kabupaten Malang, Jawa Timur. Teknik pengumpulan data dilakukan melalui observasi langsung kondisi infrastruktur jaringan, wawancara dengan pihak sekolah dan staf IT, serta dokumentasi hasil uji coba dan evaluasi performa sistem setelah implementasi. Adapun tahapan metode pelaksanaan PPM, ditunjukkan pada Gambar 1.

Gambar 1. Tahapan Metode Pelaksanaan PPM



Dengan tahapan metode pelaksanaan yang terencana, PPM ini akan memberikan kontribusi nyata dalam upaya meningkatkan keamanan jaringan komputer di SMA Islam Kepanjen.

4. HASIL DAN PEMBAHASAN

Pelaksanaan program PPM ini dilakukan berdasarkan dengan tahapan yang telah dirancang sebelumnya, mencakup survei lokasi, desain topologi jaringan, instalasi dan konfigurasi firewall, audit keamanan, pelatihan teknis, serta pendampingan.

4.1. Hasil Pengabdian

a. Instalasi dan Konfigurasi Firewall Berbasis *Wazuh*

Tim PPM berhasil melakukan instalasi dan konfigurasi sistem *Wazuh* pada server yang tersedia di laboratorium komputer SMA Islam Kepanjen. Infrastruktur jaringan yang sebelumnya tidak tersegmentasi kini dilengkapi dengan firewall aktif yang mampu memantau aktivitas jaringan secara real-time, mendeteksi intrusi, serta menghasilkan log keamanan yang dapat dianalisis oleh tim IT sekolah. Integrasi dengan *Elastic Stack* memungkinkan visualisasi data log dalam format dashboard yang mudah dipahami.

b. Audit Keamanan Jaringan

Audit keamanan dilakukan dua kali, yaitu sebelum dan sesudah implementasi firewall. Hasil menunjukkan bahwa jumlah ancaman eksternal yang terdeteksi menurun setelah penggunaan *Wazuh*, seperti ditampilkan pada Tabel 2.

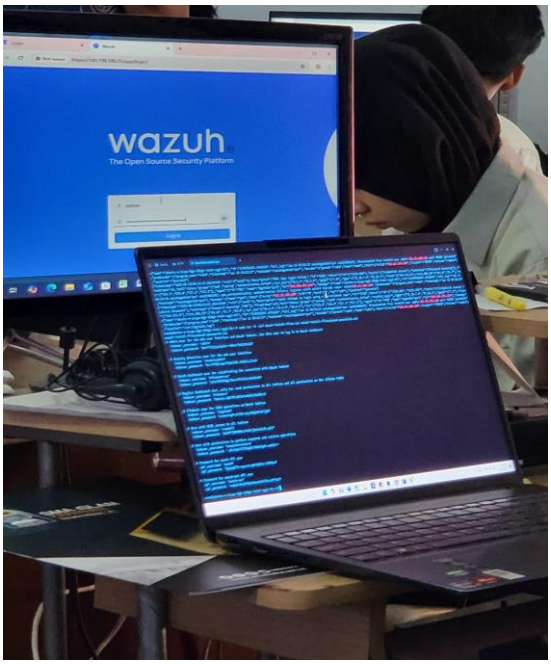
Tabel 2. Perbandingan Jumlah Ancaman Sebelum dan Setelah Implementasi Firewall

No	Aktivitas	Sebelum Implementasi Firewall	Setelah Implementasi Firewall
1	Port Scanning	Tidak terdeteksi	Terdeteksi
2	Login Gagal	Tidak terdeteksi	Terdeteksi
3	Packet Flooding	Tidak terdeteksi	Terdeteksi

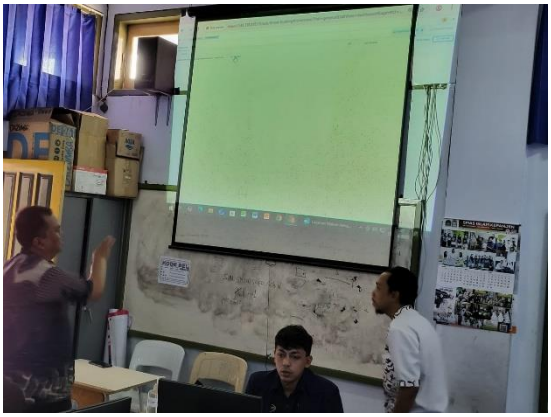
c. Pelatihan dan Pendampingan Teknis

Pelatihan teknis dilakukan dalam dua sesi selama satu minggu, diikuti staf IT SMA Islam Kepanjen. Materi mencakup konsep dasar firewall, instalasi dan konfigurasi Wazuh, analisis log, serta respons insiden. Adapun pelatihan teknis ditunjukkan pada Gambar 2, Gambar 3 dan Gambar 4.

Gambar 2. Diksusi TIM PPM dan Mitra

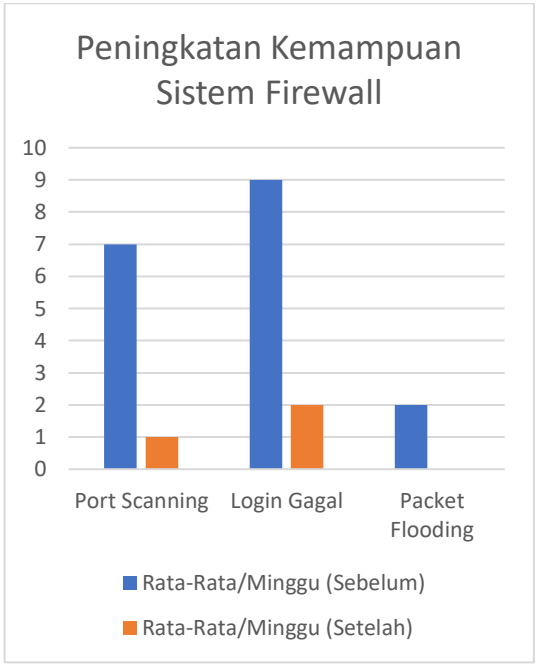


Gambar 3. Instalasi dan Konfigurasi Wazuh



Gambar 4. Implementasi Dasboard Wazuh

Hasil evaluasi setelah pelaksanaan program PPM menunjukkan adanya peningkatan kemampuan sistem firewall komputer di SMA Islam Kepanjen dalam mendeteksi berbagai serangan siber, seperti ditunjukkan pada Gambar 5



Gambar 5. Peningkatan Kemampuan Sistem Firewall

4.2. Pembahasan

a. Efektivitas Wazuh dalam Mengurangi Ancaman Siber

Penerapan Wazuh sebagai *host-based intrusion detection system* (HIDS) terbukti efektif dalam mengurangi frekuensi ancaman siber yang masuk ke jaringan internal SMA Islam Kepanjen. Dengan adanya monitoring log secara real-time, tim IT mampu merespons potensi ancaman dengan cepat dan akurat.

b. Peningkatan Kapasitas SDM Mitra

Pelatihan teknis yang dilakukan membawa dampak langsung terhadap peningkatan kapasitas staf IT mitra. Hasil evaluasi menunjukkan bahwa tingkat pemahaman tentang firewall dan keamanan jaringan meningkat signifikan. Dengan demikian, sekolah menjadi lebih mandiri dalam mengelola keamanan jaringannya sendiri.

c. Relevansi dengan Kebutuhan Sekolah

Infrastruktur keamanan yang dibangun menggunakan *Wazuh* dinilai sangat relevan dengan kondisi dan anggaran sekolah. Solusi berbasis *open source* memberikan fleksibilitas dan biaya operasional yang rendah, sehingga cocok untuk institusi pendidikan dengan sumber daya terbatas.

d. Partisipasi Mitra dalam Proses Implementasi

Mitra menunjukkan partisipasi aktif selama proses pelaksanaan PPM, termasuk dalam survei awal, uji coba sistem, dan pelatihan teknis. Partisipasi tersebut meningkatkan *sense of ownership* terhadap sistem yang baru, sehingga diharapkan akan meningkatkan kelangsungan penggunaan sistem tersebut dalam jangka panjang.

5. SIMPULAN

Program Pengabdian kepada Masyarakat (PPM) ini berhasil meningkatkan ketahanan keamanan jaringan komputer mitra melalui implementasi sistematis dan partisipatif teknologi Wazuh sebagai solusi manajemen keamanan siber. Pendekatan tersebut tidak hanya menghadirkan infrastruktur keamanan yang memadai, tetapi juga memperkuat kapasitas internal SMA Islam Kepanjen dalam pengelolaan dan pemeliharaan firewall secara mandiri. Secara holistik, program ini memberikan kontribusi signifikan terhadap peningkatan keamanan siber di institusi pendidikan tersebut, baik melalui penguatan infrastruktur teknologi maupun peningkatan kompetensi sumber daya manusia. Hasil yang dicapai diharapkan dapat menjadi model rujukan bagi penerapan teknologi informasi yang aman dan efektif di institusi pendidikan lain, khususnya dalam konteks wilayah Kabupaten Malang..

6. ACKNOWLEDGEMENT

Kami mengucapkan terima kasih kepada Tim PPM Polinema, SMA Islam Kepanjen Kabupaten Malang selaku mitra, P3M Polinema, dan Lab Applied Informatics atas dukungan dan kolaborasi dalam pelaksanaan kegiatan pengabdian ini.

7. DAFTAR REFERENSI

Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371–379.

Amami, R., Charfeddine, M., & Masmoudi, S. (2024). Exploration of Open Source SIEM Tools and Deployment of an Appropriate Wazuh-Based Solution for Strengthening Cyberdefense. *2024 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, 1–7.

Ariyanto, Y. (2023). Single Server-Side and Multiple Virtual Server-Side Architectures: Performance Analysis on Proxmox Ve for E-Learning Systems. *Journal of Engineering and Technology for Industrial Applications*, *9*(44), 25–34. https://doi.org/10.5935/jetia.v9i44.903

Ariyanto, Y., Harijanto, B., Firdaus, V. A. H., & Arief, S. N. (2020). Performance analysis of Proxmox VE firewall for network security in cloud computing server implementation. *IOP Conference Series: Materials Science and Engineering*, *732*(1). https://doi.org/10.1088/1757-899X/732/1/012081

Ariyanto, Y., Syaifudin, Y. W., Ratsanjani, M. H., Muladawila, A. R., Fatmawati, T., Saputra, P. Y., & Setiadi, C. (2025). Cyber Threat Detection and Automated Response Using Wazuh and Telegram API. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *25*(1), 173–188. https://doi.org/10.30812/matrik.v25i1.5610

Ashiq, H., Gul, N., Haleema, N., & Hameed, U. B. A. (2024). *Cyber Anomalies Detection of using ML with Wazuh/ELK (CADM)*.

Azzahra, N. S., Tambunan, A. M., Aulia, N. N., Binarsih, A., & Saepudin, T. H. (2024). Tinjauan Literatur Tentang Ancaman Cybercrime Dan Implementasi Keamanan Siber Di Industri Perbankan. *HUMANITIS: Jurnal Homaniora, Sosial Dan Bisnis*, *2*(7), 692–700.

Bhasin, V., Kumar, S., Saxena, P. C., & Katti, C. P. (2020). Security architectures in wireless sensor networks. *International Journal of Information Technology*, *12*(1), 261–272.

Dumitrasc, V. (2023). *Anomaly Detection Through User Behaviour Analysis*. Universitat Politécnica de Catalunya.

Khan, A. W., Zaib, S., Khan, F., Tarimer, I., Seo, J. T., & Shin, J. (2022). Analyzing and Evaluating Critical Cyber Security

Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach. *IEEE Access*, *10*, 65044–65054. https://doi.org/10.1109/ACCESS.2022.3179822

Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, *4*(1). https://doi.org/10.1186/s42400-021-00077-7

Malik, P., Nautiyal, L., & Ram, M. (2022). Machine Learning for Cyber Security. In *Machine Learning for Cyber Security*. https://doi.org/10.1515/9783110766745

Moiz, S., Majid, A., Basit, A., Ebrahim, M., Abro, A. A., & Naeem, M. (2024). Security and threat detection through cloud-based Wazuh deployment. *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, 1–5.

Pérez, A., Moltó, G., Caballer, M., & Calatrava, A. (2018). Serverless computing for container-based architectures. *Future Generation Computer Systems*, *83*, 50–59. https://doi.org/10.1016/j.future.2018.01.022

Pujiantoro, M. A. R., & Nugraha, I. F. (2025). MARITIME CYBERSECURITY: TANTANGAN DALAM PENGELOLAAN INFRASTRUKTUR KABEL BAWAH LAUT PADA PERAIRAN INTERNASIONAL. *Jurnal Integrasi Pengetahuan Disiplin*, *6*(1).

Stanković, S., Gajin, S., & Petrović, R. (2022). A review of Wazuh tool capabilities for detecting attacks based on log analysis. *No Nama Agent Integrity File Added Delete Modified*, *1*.

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. *IEEE Communications Surveys & Tutorials*, *25*(3), 1748–1774.

Sun, P. J. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*,https://doi.org/10.1016/j.jnca.2020.102642