Jurnal Ilmu Komputer dan Sistem Informasi
JIKSI, Vol. 01, No. 02, Juni 2020: 92-101
Received: 8 April 2020; Revised: 29 Mei 2020; Accepted: 15 Juni 2020

Studi Literature : Etika Teknologi Informasi Dalam Menghadapi Ancaman *Malicious Insider*

Dyah Ikhtiarti

Program Magister Teknik Informatika
Universitas Bina Darma
email : ikhtiartidyah@gmail.com
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstract

The development of information technology in Indonesia is experiencing rapid progress. One of them is that currently many companies and organizations operating in Indonesia use information technology and information systems in their business processes. One of the potential risks of attacks from within the company is known as insider threats. Therefore, service providers offer strong security policies and monitoring systems detect suspicious activities. The security models used are kill chain, network development life cycle (NDLC), convolutional neural network (CNN) and recurrent unit (GRU) as well as industrial control systems (ICS). The research results show that successful infrastructure security requires human resources, technical and policy aspects, how to implement advanced security technology that can prevent malicious insider crimes early on. Take proactive action to mitigate threats and protect systems from attacks and minimize potential losses.

Kata Kunci*: Insider Threats, Malicious Insiders, Technology Information*

Abstrak

Perkembangan teknologi informasi di Indoensia mengalami kemajuan pesat. Salah satunya saat ini banyak perusahaan dan organisasi yang beroperasi di Indonesia yang menggunakan teknologi informasi dan sistem informasi dalam proses bisnisnya. Salah satu potensi resiko serangan dari dalam perusahaan yang dikenal dengan insider threatment. Oleh karena itu, penyedia layanan menawarkan kebijakan kemanan yang kuat dan sistem pemantauan mendeteksi aktivitas mencurigakan. Model keamanan yang digunakan *Kill Chain, Network Development Life Cycle* (NDLC), *Convolutional Neural Network* (CNN) dan *Recurrent Unit* (GRU) serta keamanan kontrok indusri atau *Industrial Control Systems* (ICS). Hasil penelitian menunjukkan bahwa keamanan infrastruktur yang berhasil memerlukan sumber daya manusia, aspek teknis dan kebijakan, bagaimana menerapkan teknologi keamanan canggih yang dapat mencegah kejahatan orang dalam (malicious insider) sejak dini. Mengambil tindakan proaktif untuk mengurangi ancaman dan melindungi sistem dari serangan serta meminimalkan potensi kerugian.

Kata kunci: Ancaman Orang Dalam, Informasi Teknologi, Orang Dalam Berbahaya

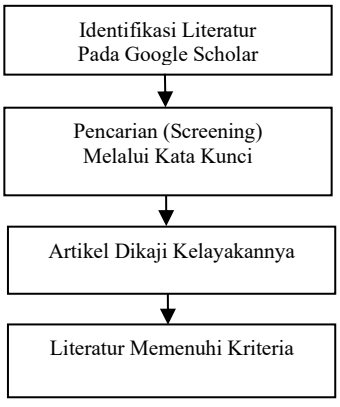
1. PENDAHULUAN

Di era yang semakin digital saat ini, tantangan keamanan siber semakin kompleks. Selain serangan eksternal seperti serangan malware dan peretasan, organisasi juga harus mewaspadai ancaman dari dalam organisasinya. Salah satu ancaman potensial dikenal sebagai ancaman orang dalam (*malicious insiders*). Hal ini karena risiko paparan orang dalam (*Malicious Insiders*) bisa sangat merugikan bisnis, memerangi ancaman orang dalam harus menjadi prioritas setiap perusahaan. Semua organisasi bisnis dan sektor bisnis merekomendasikan aktivitas bisnis dengan menggunakan internet. Komputasi *cloud* adalah kerangka kerja yang berhasil menyediakan sumber daya layanan mandiri yang cepat dan biaya terbatas di internet kepada penggunanya (Voss, 2023). Beberapa ancaman perubahan lingkungan yang serius menghadapi transisi organisasi ke cloud. Salah satu ancaman tersulit yang dihadapi suatu organisasi atau perusahaan adalah orang dalam (*Malicious Insiders*) yang berniat jahat atau orang yang berwenang mencoba mendapatkan akses informasi rahasia (Padmavathi dkk., 2022).

Lebih dari tiga perempat (77%) organisasi infrastruktur nasional penting (CNI) di AS telah mengalami ancaman siber dari dalam tiga tahun terakhir, menurut penelitian baru dari perusahaan layanan keamanan siber terkemuka Bridwell. Ancaman dari dalam berkisar dari niat kriminal hingga kelalaian individu. Namun, tindakan perusakan tersebut yang disengaja oleh karjawan rata-rata terjadi setidaknya setiap dua minggu selama setahun terakhir (Walker dkk, 2018). Tindakan yang berkaitan dengan ancaman internal dapat bersifat disengaja, seperti sabotase sistem, pencurian hak kekayaan intelektual, dan pengungkapan informasi rahasia, atau tidak disengaja seperti penggunaan sumber daya komputer secara kelalaian (Rizvi dan Williams, 2024). Tujuan utama kejahatan orang dalam (*Malicious Insider*) adalah menyebabkan kerusakan finansial dan reputasi dengan membocorkan informasi sensitif ke organisasi pesaing (Nathezhtha dkk., 2023; Alzaabi dan Mehmood, 2024). Pelaku ancaman yang canggih bersedia mengeksploitasi kerentanan dan kesalahan manusia, risiko internal melalui pemeriksaan latar belakang secara berkala, pemantauan ketat dan kontrol akses, serta pendidikan dan pelatihan keamanan siber karyawan yang berkelanjutan atas ancaman yang semakin berkembang (Aslan dkk., 2023; Moneva dan Leukfeldt, 2023). Oleh karena itu, penting untuk mendeteksi ancaman orang dalam yang berbahaya dalam suatu organisasi. Salah satu cara untuk mengidentifikasi kejahatan orang dalam dengan menganalisis perilaku pengguna (Pangesti, 2020).

2. METODOLOGI PENELITAN

Metode penelitian yang digunakan adalah studi literatur yang berfokus pada analisis literatur relevan dari lima tahun terakhir, dengan sumber utama pencarian adalah Google Scholar. Proses seleksi literatur dilakukan secara sistematis melalui empat tahapan utama.



Gambar 1: Flow Diagram Penelitian

2.1 Identifikasi Literatur Pada Google Scholar

Tahap awal dalam metodologi ini adalah Identifikasi Literatur Pada Google Scholar, yang merupakan proses pengumpulan data mentah. Peneliti memulai dengan mengakses database Google Scholar, yang berfungsi sebagai sumber utama literatur ilmiah. Dalam tahap ini, peneliti memasukkan serangkaian kata kunci yang telah dirancang untuk mencakup topik *"malicious insider"* dari berbagai sudut pandang mulai dari teknis hingga etis dan membatasi hasil pencarian hanya pada publikasi yang diterbitkan antara tahun 2022 hingga 2023 untuk menjamin relevansi dan kemutakhiran. Hasil dari tahap ini adalah kumpulan awal literatur yang luas, di mana judul dan abstraknya memiliki potensi relevansi dengan penelitian.

2.2 Pencarian (Screening) Melalui Kata Kunci

Tahapan berikutnya adalah Pencarian (*Screening*) Melalui Kata Kunci, yang berfungsi sebagai penyaringan awal untuk mengurangi jumlah literatur yang tidak sesuai. Dalam tahap ini, peneliti meninjau setiap judul dan abstrak dari daftar yang diperoleh pada tahap identifikasi. Tujuannya adalah untuk mengeliminasi literatur yang pembahasannya tidak relevan dengan isu *malicious insider* dalam konteks teknologi informasi dan keamanan. Literatur yang jelas-jelas membahas ancaman eksternal atau memiliki subjek studi yang terlalu jauh akan segera dikeluarkan dari daftar.

2.3 Artikel Dikaji Kelayakannya

Setelah penyaringan awal, literatur yang tersisa kemudian memasuki tahap krusial Artikel Dikaji Kelayakannya. Pada tahap ini, peneliti wajib memperoleh dan membaca *full-text* (teks penuh) dari setiap artikel. Pengkajian ini dilakukan secara mendalam dengan menerapkan kriteria inklusi dan eksklusi yang telah ditetapkan. Kriteria inklusi akan memastikan artikel membahas aspek yang spesifik dibutuhkan (misalnya, studi kasus, pencegahan, atau motivasi), sementara kriteria eksklusi akan menyingkirkan artikel yang memiliki kelemahan metodologi, data yang cacat, atau duplikasi pembahasan, sehingga hanya literatur yang kredibel dan berkualitas tinggi yang dapat melanjutkan ke tahap akhir.

2.4 Literatur Memenuhi Kriteria

Tahap terakhir adalah Literatur Memenuhi Kriteria, yang merupakan validasi dan finalisasi set data penelitian. Literatur yang berhasil melewati proses kajian kelayakan (tahap 3) secara resmi dinyatakan sebagai literatur yang relevan dan valid untuk digunakan dalam penelitian ini. Kumpulan artikel final inilah yang akan membentuk korpus literatur utama, yang kemudian akan dianalisis, disintesis, dan dirangkum secara komprehensif dalam sub-bab Hasil dan Pembahasan untuk menjawab tujuan penelitian.

3. HASIL DAN PEMBAHASAN

Berdasarkan review maka peneliti memilih beberapa literatur sesuai dengan tema yang telah ditentukan, maka didapatkan hasil sebagai berikut:

Table 1 : Literatur Tentang Keamanan Sistem Informasi Terhadap Ancaman *Malicious Insider*

No	Nama Peneliti	Judul Penelitian	Tahun	Metode Penelitian	Hasil Penelitian
1	Dedy Hariyadi, Cici Finansia	Analisis Insider Threat Pada Sistem	2023	Menurut Lockheed Martin Corporation,	Hasil penelitian ini menunjukan ancaman serangan

		Keamanan Rumah Cerdas Menggunakan Malicious Traffic Monitoring		Industri Pertahanan yang berpusat di Amerika Serikat mengusulkan kerangka kerja untuk membatasi ruang gerak penyerang atau threat actor dengan memahami 7 tahapan perilakunya yaitu, *reconnaissance, weaponization, delivery, exploitation, installation, command & control*, dan *action on objectives (steal confidential* data) (Kumar dkk., 2021). Penelitian ini menggunakan metode pemantauan *malicious traffic* pada ekosistem rumah cerdas. Metode ini merupakan baguan memutus rantai berdasarkan model *cyber kill chain.*	siber semakin kompleks karena harus melihat dari dua sisi. Sehingga dalam proses mengamankan sistem komputer dan jaringan dari dua sisi, yaitu dari dalam dan luar ekosistem diperlukan sebuah deteksi serangan siber. Adapun bentuk atau upaya serangan dari dalam dapat disebabkan oleh aktivitas pengguna saat melakukan akses internet. Dengan pemasangan sensor lalu lintas jaringan mengunakan *MalTrail* dapat mengetahui upaya serangan siber dari sisi internal ekosistem rumah cerdas sejak dini.
2	Dedy Hariyadi, Kartikadyota Kusumaningtyas, Burhan Alfironi Muktamar	Implementasi *Malicious Traffic* Untuk Mendeteksi Serangan Siber di SMK Muhammadiyah 1 Yogyakarta	2023	*Network Development Life Cycle* (NDLC) adalah metodologi yang digunakan di bidang rekayasa dan manajemen jaringan untuk memandu proses	Potensi kebocoran data muncul dari berbagai faktor termasuk diantaranya serangan rekayasa sosial, kelemahan dalam aplikasi pihak ketiga, berbagi data,

		perencanaan, perancangan, implementasi, dan pemeliharaan sistem komputer dan jaringan yang terstruktur, sistematis, dan efisien.	ancaman orang dalam (insider threat), dan kurangnya kesadaran menjaga privasi pengguna. potensi ancaman serangan siber yang terekam diantaranya potensi kebocoran data dari pengguna ponsel. Kebocoran data yang terekam diantaranya IMEI dan model ponsel yang dikirimkan oleh pengguna secara tidak sadar saat mengakses situs web. Dampak dari kebocoran data adalah pemilik situs web dapat mengetahui ada ponsel dengan IMEI dan model tertentu sedang mengakses situs web. Bahkan pemilik situs web dapat mengetahui IP Address pengakses melalui fitur GeoIP, yaitu teknologi yang digunakan untuk mengetahui geolokasi dengan menentukan lokasi geografis host internet berdasarkan alamat IP. Pada implementasi sensor potensi ancaman serangan siber mengggunakan *MalTrail* belum

					terintegrasi dengan firewall.
3.	Olarotimi Kabir Amuda, Bodunde Odunola Akinyemi , Mistura Laide Sanni and Ganiyu Adesola Aderounmu	A Predictive User Behaviour Analytic Model for Insider Threats in Cyberspace	2022	Metode penelitian ini *Convolutional Neural Network* (CNN) *and Gated Recurrent Unit* (GRU). digunakan untuk menentukan apakah pengguna perilaku tersebut cenderung berbahaya dan akibatnya menentukan prediksi ancaman komprehensif di log pengguna kumpulan data file.	Hasil dari Simulasi menunjukkan bahwa model yang dikembangkan mengalami peningkatan sebesar Akurasi deteksi 1,48%, presisi 4,21%, dan 1,25% sensitivitas terhadap model yang ada. Hal ini menunjukkan bahwa pendekatan hybrid yang dikembangkan mampu belajar dari rangkaian tindakan pengguna dalam domain waktu dan frekuensi dan meningkatkan tingkat deteksi ancaman orang dalam di dunia maya.
4.	Bakil Al-Muntaser, Mohamad Afendee Mohamed, Ammar Yaseen Tuama	*Real-Time Intrusion Detection of Insider Threats in Industrial Control System Workstations Through File Integrity* Monitoring	2023	Model yang digunakan dalam penelitian ini yaitu *Industrial control systems* atau Sistem kendali industri (ICS). Memastikan keamanannya adalah hal yang terpenting untuk menjaga kontinuitas dan keandalan proses.	Melalui ekstensif pengujian, model mencapai tingkat akurasi yang tinggi, mendeteksi intrusi orang dalam dengan tingkat positif sebenarnya yang tinggi. Ini dapat diandalkan kemampuan deteksi berkontribusi untuk meningkatkan keamanan ICS dan memitigasi risiko yang terkait

	dengan ancaman orang dalam. Oleh menerapkan sistem deteksi intrusi *real-time* ini, organisasi dapat secara efektif melindungi sistem pengendaliannya menjaga privasi pengguna.

Ancaman serangan siber tidak hanya datang dari luar, (Hariyadi dan Finansia, 2023) menunjukkan bahwa ancaman serangan siber juga ada di dalam sistem komputer dan jaringan internal. Artinya ancaman serangan siber dapat diklarifikasikan berdasarkan sumber ancamannya, sehingga terbagi menjadi dua, yaitu ancaman internal dan ancaman eksternal. Hal ini menunjukkan bahwa ancaman serangan siber semakin kompleks karena harus dilihat dari dua sisi. Bentuk upaya serangan orang dalam dapat diakibatkan oleh aktivitas pengguna saat menggunakan internet. Dengan memasang sensor lalu lintas jaringan dengan *MalTrail*, dapat mendeteksi serangan siber sejak dini di ekosistem rumah pintar. Resiko serangan siber terhadap perangkat pintar atau perangkat LoT tidak terbukti dalam penelitian ini. Pada penelitian (Hariyadi dkk., 2023) menyatakan untuk mengidentifikasi serangan siber intranet dilakukan dengan memasang sensir pemantau lalu lintas yang tidak biasa. Menciptakan beberapa potensi. Potensi ancaman serangan siber yang tercatat antara lain potensi kebocoran data dari posel pengguna. Aliran data direkam mencakup IMEI dan model tertentu yang masuk ke situs tersebut. Bahkan pemilik *website* dapat mengetahu alamat IP pengguna menggunakan fitur GeoIP, yang digunakan untuk geolokasi dengan menentukan lokasi geografis host internet berdasarkan alamat IP. Penyebaran sensor belum mengintegrasikan *firewall* untuk menghadapi potensi ancaman serangan siber *MalTrail*.

Penelitian Amuda dkk., 2022 ini berfokus pada mengidentifikasi ancaman orang dalam di dunia maya menggunakan analisis perilaku pengguna. Model saat ini dihadapkan pada ketidakmampuannya mendeteksi perilaku yang tidak diketahui atau bersifat sementara, sehingga menyebabkan beberapa prrilaku pengguna yang tidak wajar dan tidak diketahui. Selain itu, sebagian besar model yang ada tidak dapat belajar dari siklus perilaku pengguna, sehingga menghasilkan tingkat deteksi yang rendah dan tingkat alarm palsu tinggi (Liu & Lang, 2019; Riza, 2023). Studi ini mengembangkan teknologi hybrid insider ancaman model dengan pembelajaran mendalam untuk meningkatkan deteksi ancaman orang dalam di dunia maya. Hasil simulasi menunjukkan bahwa model diusulkan dapat mendeteksi lebih dari ancaman internal dan memiliki tingkat akurasi deteksi, presisi, dan sensitivitas yang lebih tinggi dibandingkan model individu LTSM, GRU, dan CNN yang ada. Ia juga memiliki kemampuan untuk mempelajari urutan data pengguna, sehingga menghasilkan tingkat deteksi yang lebih cepat ketika GRU dan CNN individual ada. Penelitian dari (Al-Muntaser dkk., 2023) yang menerapkan pemantauan integritas file telah terbukti menjadi metode yang efektif dan akurat untuk mendeteksi intrusi internal yang melibatkan kerusakan file pada stasiun kerja sistem kontrol. Pelanggaran ini meliputi kerusakan data, perusakan data, modifikasi tanpa izin, injeksi kode berhahaya, modifikasi data yang tidak sengaja. Model juga memfasilitasi pendeteksian jenis serangan lain yang melibatkan perubahan pada konten file seperti ransomware dan eksekusi kode jarak jauh. Proses identifikasi dilakukan tanpa perlu memantau perilaku dan tindakan pengguna, sehingga menjada privasi pengguna. Meskipun model yang diselidiki dalam penelitian ini menunjukkan efektivitas dalam mendeteksi ancaman internal yang terkait dengan pelanggaran integritas file. Model tersebut tidak memiliki kemampuan untuk mendeteksi ancaman internal lainnya yang menyebabkan perubahan pada

konten file, seperti pencurian aset. Informasi intelektual dan tidak sah. Mengakses menjelajahi dan mengatasi ancaman orang dalam tambahan ini mungkin merupakan bidang yang menjanjikan untuk penelitian di masa depan. Aspek penting lainnya dari yang perlu diperhatikan bahwa model hanya berfokus pada deteksi intrusi dan tidak memiliki kemampuan untuk mencegah konsekuensinya secara mandiri. Oleh karena itu, untuk efektivitas maksimum penting untuk mengintegrasikan strategi pemantauan integritas file ke dalam rencana respons insiden organisasi. Integrasi ini memastikan tindakan yang tepat dan tepat waktu diambil untuk mengurangi pelanggaran integritas file, sehingga mencegah konsekuensi lebih lanjut yang tidak diinginkan.

Terjadinya ancaman kejahatan orang dalam (*malicious insider*) dengan tingginya tingkat risiko yang terkait dengan faktor manusia, seperti ketakutan, kesalahan, atau pelatihan yang tidak memadai, penelitian ini menyoroti perlunya organisasi untuk sangat waspada terhadap ancaman dari dalam dan karyawan yang rentan seiring dengan pemulihan perekonomian dan negara-negara yang masih terikat secara politik. Deteksi intrusi jaringan, firewall, dan sistem anti-virus telah terbukti tidak efektif dalam mendeteksi serangan orang dalam. Pusat keamanan besar telah mulai menerapkan sensor berbasis titik akhir yang memberikan organisasi mereka visibilitas yang lebih besar terhadap peristiwa tingkat rendah (Berlin dkk., 2015). Pada artikel di atas belum ditemukan framework yang tepat untuk kemanan terhadap ancaman kejahatan orang dalam (*malicious insider*). Orang dalam yang jahat adalah seseorang yang dengan jahat dan sengaja menyalahgunakan kredensial yang sah, biasanya untuk mencuri informasi demi insentif keuangan atau pribadi. Contohnya adalah pekerja yang menyimpan dendam terhadap mantan majikannya atau pekerja oportunis yang menjual informasi rahasia kepada pesaing. Orang dalam yang jahat memiliki keunggulan dibandingkan penyerang lainnya karena mereka memahami kebijakan dan prosedur keamanan organisasi serta kerentanannya (Gheyas & Abdallah, 2016). Solusi menghadapi ancaman kejahatan orang dalam (*malicious insider*). Analisis perilaku pengguna dengan mendapatkan visibilitas terhadap anomali perilaku yang mungkin menandakan ancaman aktif dari dalam, manajemen akses istimewa lokal atau di cloud, uji sumber daya manusia dengan simulasi musuh, penyetelan kontrol maupun layanan rekayasa sosial, dan perlindungan data dari ransomware atau malware jahat yang dapat menyandera organisasi.

4. KESIMPULAN

Ancaman serangan siber dapat diklarifikasikan berdasarkan sumber ancamannya, bentuk upaya serangan orang dalam dapat diakibatkan oleh aktivitas pengguna saat menggunakan internet. Dengan memasang sensor lalu lintas jaringan dengan *MalTrail*, dapat mendeteksi serangan siber sejak dini. Dengan memasang sensor lalu lintas jaringan dengan *MalTrail*, tetapi penyebaran sensor belum mengintegrasikan *firewall* untuk menghadapi potensi ancaman serangan siber *MalTrail*. Hasil simulasi menunjukkan bahwa model diusulkan dapat mendeteksi lebih dari ancaman internal dan memiliki tingkat akurasi deteksi, presisi, dan sensitivitas yang lebih tinggi dibandingkan model individu LTSM, GRU, dan CNN yang ada. Ia juga memiliki kemampuan untuk mempelajari urutan data pengguna, sehingga menghasilkan tingkat deteksi yang lebih cepat ketika GRU dan CNN individual ada. Mendeteksi ancaman internal yang terkait dengan pelanggaran integritas *file*, proses identifikasi dilakukan tanpa perlu memantau perilaku dan tindakan pengguna, sehingga menjada privasi pengguna. Meskipun model yang diselidiki dalam penelitian ini menunjukkan efektivitas dalam mendeteksi ancaman internal yang terkait dengan pelanggaran integritas file. Model tersebut tidak memiliki kemampuan untuk mendeteksi ancaman internal lainnya yang menyebabkan perubahan pada konten file, seperti pencurian aset. Informasi intelektual dan tidak sah. Mengakses menjelajahi dan mengatasi ancaman orang dalam tambahan ini mungkin merupakan bidang yang menjanjikan untuk penelitian di masa depan.

Referensi

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, *31*(3), 875-888.

Al-Muntaser, B., Mohamed, M. A., & Tuama, A. Y. (2023). Real-Time Intrusion Detection of Insider Threats in Industrial Control System Workstations Through File Integrity Monitoring. *International Journal of Advanced Computer Science and Applications*, *14*(6). https://doi.org/10.14569/IJACSA.2023.0140636

Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access, 12, 30907-30927.

Amuda, O. K., Akinyemi, B. O., Sanni, M. L., & Aderounmu, G. A. (2022). A PREDICTIVE USER BEHAVIOUR ANALYTIC MODEL FOR INSIDER THREATS IN CYBERSPACE. *International Journal of Communication Networks and Information Security (IJCNIS)*, *14*(1). https://doi.org/10.17762/ijcnis.v14i1.5208

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

Berlin, K., Slater, D., & Saxe, J. (2015). Malicious Behavior Detection using Windows Audit Logs. *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*, 35–44. https://doi.org/10.1145/2808769.2808773

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1), 6. https://doi.org/10.1186/s41044-016-0006-0

Hariyadi, D., & Finansia, C. (2023). Analisis Insider Threat pada Sistem Keamanan Rumah Cerdas Menggunakan Malicious Traffic Monitoring. *Jurnal Aplikasi Teknologi Informasi Dan Manajemen (JATIM)*, *4*(2), 107–114. https://doi.org/10.31102/jatim.v4i2.2287

Hariyadi, D., Kusumaningtyas, K., & n Alfironi Muktamar, B. (2023). Implementasi Malicious Traffic Untuk Mendeteksi Serangan Siber di SMK Muhammadiyah 1 Yogyakarta. *Jurnal INTEK*, *6*(2), 73–78.

Kumar, R., Singh, S., & Kela, R. (2021). A Quantitative Security Risk Analysis Framework for Modelling and Analyzing Advanced Persistent Threats. In G. Nicolescu, A. Tria, J. M. Fernandez, J.-Y. Marion, & J. Garcia-Alfaro (Eds.), *Foundations and Practice of Security* (pp. 29–46). Springer International Publishing. https://doi.org/10.1007/978-3-030-70881-8_3

Liang, N., Biros, D. P., & Luse, A. (2023). An empirical comparison of malicious insiders and benign insiders. *Journal of Computer Information Systems*, 1-13.

Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. applied sciences, 9(20), 4396.

Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. IEEE Access, 6, 25167-25177.

Moneva, A., & Leukfeldt, R. (2023). Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. *Journal of Criminology*, *56*(4), 416-440.

Nathezhtha, T., Sangeetha, D., & Vaidehi, V. (2023). Social network malicious insider detection using time-based trust evaluation. *Annals of Telecommunications*, 1-13

Padmavathi, G., Shanmugapriya, D., & Asha, S. (2022, May). A Framework for Improving the Accuracy with Different Sampling Techniques for Detection of Malicious Insider Threat in Cloud. In *Proceedings of International Joint Conference on Advances in*

Computational Intelligence: IJCACI 2021 (pp. 485-494). Singapore: Springer Nature Singapore.

Pangesti, N. (2020). Studi Literatur: Pengaruh Pelatihan Interprofesional Terhadap Self Eficacy Pada Mahasiswa Kesehatan. *Dinamika Kesehatan Jurnal Kebidanan Dan Keperawatan*, *10*, 328–339. https://doi.org/10.33859/dksm.v10i1.395

Riza, F. (2023). Sistem deteksi intrusi pada server secara realtime menggunakan seleksi fitur dan firebase cloud messaging. Jurnal Sistim Informasi dan Teknologi, 7-15.

Rizvi, S., & Williams, I. (2024). Analyzing transparency and malicious insiders prevention for cloud computing environment. *Computers & Security*, *137*, 103622.

Voss, E. (2023). *Insider Threat: A Case Study, Recognizing the Early Warnings Signs by Humans* (Doctoral dissertation, Northcentral University).