Jurnal Impresi Indonesia (JII)
p-ISSN: 2828-1284 e-ISSN: 2810-062x
Vol. 5. No. 5. 2026

Penerapan IBM Qradar Security Information and Event Management (SIEM) Untuk Deteksi Ancaman Keamanan Jaringan Pada Infrastruktur Job Tomori

Muhammad Aydin Rafif Reyfan*, Oky Tria Saputra
Politeknik IDN, Indonesia
Email: aydinrafif48@gmail.com*, okytria@gmail.com

Keywords:
network security; qradar; siem; threat detection.

Abstract
This study discusses the implementation of IBM QRadar Security Information and Event Management (SIEM) in supporting network monitoring and threat detection processes. As network infrastructures continue to grow, the volume of logs and recorded activities also increases, making manual analysis using conventional methods inefficient. Therefore, a system capable of managing and analyzing data in a centralized manner is required. The method used in this study includes the installation and configuration of QRadar in a simulated network environment, integration of various log sources such as servers, firewalls, and routers, and the creation of correlation rules to identify suspicious activity patterns. The observation process was conducted to evaluate the system's ability to detect several types of threats, such as repeated login attempts, unauthorized access, and abnormal traffic activities. The results show that QRadar is capable of processing large volumes of log data and presenting information in the form of real-time alerts and dashboard visualizations. This capability helps administrators identify potential threats more quickly and take appropriate actions. Overall, the use of QRadar-based SIEM improves the effectiveness of network security monitoring.

Kata Kunci:
network security; qradar; siem; threat detection.

Abstrak
Penelitian ini membahas penerapan IBM QRadar Security Information and Event Management (SIEM) dalam mendukung proses monitoring dan deteksi ancaman pada jaringan. Seiring dengan berkembangnya infrastruktur jaringan, jumlah log dan aktivitas yang tercatat juga semakin besar, sehingga sulit dianalisis secara manual menggunakan metode konvensional. Oleh karena itu, dibutuhkan sistem yang mampu mengelola dan menganalisis data secara terpusat. Metode yang digunakan dalam penelitian ini meliputi instalasi dan konfigurasi QRadar pada lingkungan jaringan uji, integrasi berbagai sumber log seperti server, firewall, dan endpoint, serta pembuatan aturan korelasi untuk mengidentifikasi pola aktivitas yang mencurigakan. Proses pengamatan dilakukan untuk melihat kemampuan sistem dalam mendeteksi beberapa jenis ancaman, seperti percobaan login berulang, akses tidak sah, dan aktivitas lalu lintas yang tidak normal. Hasil penelitian menunjukkan bahwa QRadar mampu mengolah data log dalam jumlah besar dan menyajikan informasi dalam bentuk notifikasi serta tampilan dashboard secara real-time. Hal ini membantu administrator dalam mengenali potensi ancaman lebih cepat dan mengambil tindakan yang diperlukan. Secara keseluruhan, penggunaan SIEM berbasis QRadar dapat meningkatkan efektivitas pemantauan keamanan

PENDAHULUAN

Cara perusahaan mengelola dan melindungi infrastruktur jaringan mereka telah sangat dipengaruhi oleh perkembangan teknologi informasi yang semakin pesat (Anggraeni & Maulani, 2023; Hoshmand & Ratnawati, 2023; Nabila et al., 2025; Sani et al., 2025). Di era digital, data menjadi aset yang sangat penting, jadi sangat penting untuk menjaga keamanan jaringan (Aulia et al., 2023; Chic & Bilqisthi, 2024; Prasetia et al., 2024; Tommy & Nasution, 2025; Yonatan et al., 2024). *Malware, phishing, ransomware, dan serangan Distributed Denial of Service (DDoS)* adalah contoh ancaman siber yang semakin kompleks. Ini berarti bahwa sistem keamanan harus ada yang dapat mendeteksi, menganalisis, dan merespons ancaman secara cepat dan tepat.

Sebagai infrastruktur teknologi yang mendukung berbagai aktivitas operasional seperti oil and gas, JOB Tomori menghadapi tantangan besar dalam menjaga integritas, kerahasiaan, dan ketersediaan data (Stergiopoulos et al., 2020). Potensi serangan siber meningkat karena jumlah lalu lintas jaringan dan aplikasi yang digunakan (Mohammed et al., 2022; Yadav & Paul, 2021). Akibatnya, solusi keamanan yang komprehensif diperlukan untuk memantau aktivitas jaringan secara real time, menemukan pola serangan, dan memberikan peringatan dini terhadap ancaman yang mungkin terjadi (Fausto et al., 2021; Alanazi et al., 2023).

Untuk mengatasi kebutuhan tersebut, *IBM QRadar Security Information and Event Management (SIEM)* dapat mengintegrasikan berbagai sumber log dan data keamanan, kemudian melakukan analisis korelasi untuk menemukan aktivitas mencurigakan. Dengan fitur *real-time monitoring*, *threat intelligence*, serta kemampuan *incident response*, Teknologi ini diharapkan dapat melindungi infrastruktur Job Tomori lebih baik dan memastikan operasi lancar tanpa gangguan siber.

Penelitian ini akan membahas penerapan *IBM QRadar Security Information and Event Management (SIEM)* untuk mendeteksi ancaman keamanan jaringan pada infrastruktur Job Tomori dan memastikan kelancaran operasional tanpa terganggu oleh ancaman siber. Fokus utama adalah bagaimana sistem ini dapat digunakan dan sejauh mana hal itu membantu meningkatkan keamanan jaringan dan mengurangi potensi serangan siber.

Beberapa penelitian terdahulu yang relevan dengan topik penerapan Security Information and Event Management (SIEM), khususnya IBM QRadar, dalam mendeteksi ancaman keamanan jaringan adalah sebagai berikut: 1) Suskalo, D., Moric, Z., Redzepagic, J., & Damir Regvart. (2023) melakukan comparative analysis tentang IBM QRadar dan Wazuh untuk Security Information and Event Management (SIEM) (González-Granadillo et al., 2021). Tujuan dari makalah ini adalah untuk melakukan analisis perbandingan antara dua alat Security Information and Event Management (SIEM) terkemuka: IBM QRadar Security Information and Event Management (SIEM) yang komersial dan Wazuh solusi keamanan sumber terbuka (Winkler et al., 2025; Safarzadeh et al., 2024). Fokus utama yang dipilih adalah untuk mengevaluasi sejauh mana alat-alat ini dapat memenuhi persyaratan keamanan dalam infrastruktur IT yang tipikal. 2) Seppänen, M. (2021) melakukan studi evaluasi tentang UEBA dari sudut pandang Security Operations Center (SOC). Salah satu tantangan yang dihadapi Security Operations Center (SOC) adalah kebutuhan yang terus-menerus untuk mengembangkan metode deteksi insiden keamanan dalam lanskap ancaman yang terus berkembang dan volume data yang semakin besar yang perlu diproses (Carrera et al., 2024). Pengambilan data log mentah oleh Security Information and Event Management (SIEM) merupakan contoh utama data streaming yang melampaui kemampuan otomatisasi tradisional

dan analis manusia (Muhammad et al., 2023). 3) Putra, W. P., Burjulius, R., Al Hilmi, M. A., & Sumarudin, A. (2024) meneliti penerapan Security Information and Event Management (SIEM), khususnya Wazuh Security Information and Event Management (SIEM), sebagai sistem peringatan dini untuk mendeteksi dan menanggulangi serangan server, terutama serangan Distributed Denial of Service (DDoS). Sistem memberikan visibilitas dan kontrol keamanan yang lebih besar, serta respons real time terhadap ancaman (Nandaputra et al., 2024). 4) Khotimah, H., Bimantoro, F., & Kabanga, R. S. (2022) menerapkan sistem SIEM (Security Information and Event Management) berbasis Wazuh pada aplikasi SMS Center milik Pemerintah Provinsi Nusa Tenggara Barat, untuk mempermudah monitoring dan analisis keamanan serta mendeteksi serangan siber yang mengancam sistem (Bezas & Filippidou, 2024).

Berdasarkan latar belakang yang telah diuraikan, maka perumusan permasalahan yang akan dibahas dalam Tugas Akhir ini adalah sebagai berikut: 1) Penelitian ini menelaah penerapan *IBM QRadar Security Information and Event Management (SIEM)* dalam mendeteksi ancaman keamanan jaringan pada infrastruktur Job Tomori, dengan fokus pada kapabilitas utama seperti *scalability, security, reliability, simplicity of management, agility*, serta *network visibility*. 2) Analisis dilakukan untuk menilai sejauh mana *IBM QRadar Security Information and Event Management (SIEM)* mampu mengatasi kekurangan atau keterbatasan sistem monitoring tradisional, serta mengevaluasi kelebihan dan kekurangan penerapan *Security Information and Event Management (SIEM)* dalam konteks implementasi nyata pada infrastruktur jaringan Job Tomori. 3) Studi ini mengkaji kesesuaian desain, kapabilitas, dan implementasi *IBM QRadar Security Information and Event Management (SIEM)* dalam mendukung kebutuhan mendeteksi ancaman modern yang dinamis, serta tingkat kompatibilitasnya terhadap tuntutan *agility, security*, dan *automation* yang dibutuhkan oleh organisasi. 4) Hasil analisis penerapan *IBM QRadar Security Information and Event Management (SIEM)* dijadikan dasar untuk merumuskan rekomendasi penguatan sistem keamanan jaringan pada Job Tomori, dengan menyoroti *lessons learned* serta gap antara desain aktual dan *best practices* dari *IBM QRadar Security Information and Event Management (SIEM)*.

Berdasarkan rumusan masalah, tujuan dari penyusunan Tugas Akhir ini adalah: 1) Menganalisis dan mengevaluasi secara komprehensif kapabilitas utama *IBM QRadar Security Information and Event Management (SIEM)*, meliputi *scalability, security, reliability, simplicity of management, agility*, serta *network visibility*, dalam konteks penerapan pada infrastruktur jaringan Job Tomori. 2) Mengidentifikasi kelebihan, kekurangan, dan *trade offs* dari penerapan *IBM QRadar Security Information and Event Management (SIEM)* dibandingkan dengan sistem monitoring tradisional, berdasarkan studi kasus implementasi nyata di Job Tomori. 3) Mengevaluasi kesesuaian desain dan implementasi *IBM QRadar Security Information and Event Management (SIEM)* terhadap *best practices* resmi *IBM*, serta mengidentifikasi *gap* dan peluang optimasi dalam mendukung kebutuhan deteksi ancaman modern. 4) Memberikan rekomendasi praktis dan *actionable insights* bagi administrator jaringan, tim *IT Security*, maupun pengambil keputusan di Job Tomori dalam konteks desain, implementasi, dan penguatan sistem keamanan jaringan berbasis *Security Information and Event Management (SIEM)*.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan **kualitatif deskriptif** dengan metode **studi kasus** dan teknik ***design evaluation*** untuk menganalisis penerapan *IBM QRadar Security Information and Event Management (SIEM)* dalam mendeteksi ancaman keamanan jaringan.

Metode dan Tahapan Analisis

1. Studi Literatur dan Benchmarking *(Literature Review)*
   a. Mengumpulkan referensi terkait konsep *Security Information and Event Management (SIEM)*, arsitektur keamanan jaringan, serta *IBM QRadar* dari jurnal, whitepaper resmi *IBM*, dokumentasi teknikal, dan studi kasus terdahulu.
   b. Mengidentifikasi praktik terbaik dan prinsip desain dalam penerapan *Security Information and Event Management (SIEM)*, khususnya terkait kapabilitas utama yang menjadi fokus penelitian: *scalability, security, reliability*, dan sederhananya menggunakan sistem informasi.
2. Deskripsi Kasus dan Pengumpulan Data
   a. Mengumpulkan data dari dokumentasi konfigurasi sistem, log keamanan, *topology diagrams*, serta hasil observasi aspek operasional jaringan Job Tomori.
   b. Melakukan wawancara atau diskusi dengan tim *IT/security* Job Tomori, agar memperoleh informasi terkait kebutuhan, kendala, dan pengalaman implementasi.
   c. Semua data bersifat sensitif saat penelitian akan dianonimkan sesuai kebijakan kerahasiaan dan etika penelitian.
3. Penentuan Kriteria Evaluasi

Mendefinisikan kapabilitas utama sebagai dimensi evaluasi penerapan *QRadar Security Information and Event Management (SIEM)*:

   a. ***Scalability***: Sistem karantina, fleksibilitas integrasi log, dan dukungan pertumbuhan *endpoint*.
   b. ***Security***: Model keamanan penerapan kebijakan granular, deteksi ancaman dan dukungan terhadap konsep *Zero Trust*.
   c. ***Reliability***: Redundansi, *tolerance error*, jaminan *uptime*, dan *failover*.
   d. ***Simplicity of Management dan Agility***: Pengelolaan terpusat, level otomatisasi, *ease provision*, dan kompleksitas *troubleshooting*.
   e. ***Network Visibility***: Kemampuan sistem dalam memberikan visibilitas menyeluruh terhadap perangkat, aktivitas jaringan, serta *endpoint virtual (VM, container)*.
4. Analisis Implementasi
   a. Melakukan Analisis penerapan *IBM QRadar Security Information and Event Management (SIEM)* pada infrastruktur Job Tomori berdasarkan dimensi evaluasi yang telah ditentukan.
   b. Mendokumentasikan kelebihan, kekurangan, trade-offs, dan implikasi praktis dari setiap aspek.
   c. Menggunakan tabel evaluasi dan visualisasi untuk memperjelas hasil analisis.
5. Rekomendasi
   a. Membuat rekomendasi berdasarkan hasil analisis dan pelajaran yang dipelajari dari implementasi *QRadar Security Information and Event Management (SIEM)*.
   b. Menampilkan praktik terbaik untuk implementasi *QRadar SIEM* yang dapat digunakan oleh Job Tomori maupun organisasi lain dalam penguatan sistem keamanan jaringan.

HASIL DAN PEMBAHASAN

Deskripsi Studi Infrastruktur JOB Tomori

Infrastruktur jaringan dan keamanan JOB Tomori merupakan lingkungan operasional berskala enterprise yang digunakan sebagai objek penelitian dalam penerapan IBM QRadar Security Information and Event Management (SIEM). Lingkungan ini berfungsi sebagai studi kasus nyata (field laboratory) yang memungkinkan peneliti melakukan observasi langsung terhadap proses pengumpulan log, korelasi ancaman, serta efektivitas deteksi keamanan dalam kondisi produksi.

JOB Tomori mengoperasikan berbagai perangkat keamanan dan jaringan seperti firewall, IDS/IPS, router, server, dan aplikasi kritikal yang menghasilkan ribuan log setiap hari. Sebelum penerapan SIEM, log dari perangkat-perangkat tersebut masih terpisah (siloed) sehingga menyulitkan proses monitoring dan deteksi ancaman secara menyeluruh.

Implementasi IBM QRadar SIEM dilakukan untuk:

1. Mengintegrasikan seluruh log source ke dalam satu platform terpusat
2. Melakukan normalisasi dan korelasi log secara otomatis
3. Meningkatkan visibilitas keamanan jaringan
4. Mendeteksi ancaman secara real-time
5. Mempercepat proses investigasi insiden

Lingkup Infrastruktur JOB Tomori

Lingkungan penelitian mencakup beberapa area operasional yang saling terhubung, yaitu:

Lokasi Operasional Utama

Merupakan pusat aktivitas jaringan dan keamanan, tempat sebagian besar perangkat kritikal berada, termasuk firewall utama, server aplikasi, dan perangkat jaringan inti.

Lokasi Pendukung / Secondary Site

Digunakan untuk layanan operasional tambahan dan redundansi sistem. Perangkat di lokasi ini juga menjadi sumber log yang diintegrasikan ke QRadar.

Sistem Monitoring dan Keamanan

Sebelum implementasi QRadar, sistem monitoring masih bersifat manual dan terfragmentasi. Setelah implementasi, seluruh log dari berbagai lokasi dikumpulkan dan dianalisis secara terpusat melalui QRadar.

Karakteristik Lingkungan Penelitian

Enterprise-scale

Infrastruktur terdiri dari berbagai perangkat keamanan dan jaringan yang menghasilkan volume log besar dan beragam.

Multi-unit Operations

Mendukung berbagai fungsi operasional perusahaan yang membutuhkan tingkat keamanan tinggi.

Operational Maturity

Sistem telah berjalan dalam kondisi produksi selama bertahun-tahun sehingga menyediakan data operasional yang valid untuk dianalisis.

Real-world Complexity

Lingkungan nyata memungkinkan peneliti menangkap pola ancaman, anomali, dan aktivitas jaringan yang tidak dapat disimulasikan secara akurat di laboratorium buatan.

Keuntungan Menggunakan Lingkungan Nyata

Kondisi Real-time

Memberikan gambaran autentik mengenai ancaman yang terjadi di lingkungan operasional JOB Tomori.

Data Empiris:

Analisis dilakukan berdasarkan log aktual, offense QRadar, dan aktivitas jaringan nyata.

Relevansi Praktis:

Hasil penelitian dapat langsung diterapkan untuk meningkatkan keamanan jaringan perusahaan.

Constraint Realism:

Penelitian mempertimbangkan keterbatasan operasional, kebijakan internal, dan kebutuhan bisnis yang sesungguhnya.

Deskripsi Arsitektur

Arsitektur Keamanan Existing JOB Tomori

Arsitektur keamanan existing di JOB Tomori sebelumnya menggunakan pendekatan tradisional, di mana setiap perangkat keamanan dan jaringan bekerja secara terpisah (siloed) tanpa adanya platform terpusat untuk korelasi log dan deteksi ancaman.

Lingkungan ini terdiri dari beberapa komponen utama:

Perangkat Firewall

Berfungsi sebagai pengendali akses dan proteksi perimeter. Firewall menghasilkan berbagai jenis log seperti:

1. Traffic log
2. Connection log
3. Intrusion attempt log
4. NAT log

IDS/IPS

Digunakan untuk mendeteksi dan mencegah serangan berbasis signature maupun anomaly.

Log IDS/IPS mencakup:

1. Alert serangan
2. Signature match
3. Suspicious traffic pattern

Namun tidak terintegrasi dengan log perangkat lain.

Router dan Switch Core

Menghasilkan log terkait:

1. Routing changes
2. Interface status
3. Error log
4. Network anomaly

Tetapi tidak dianalisis secara terpusat.

Server Aplikasi dan Sistem Operasional

Menghasilkan:

1. Authentication log
2. System event log
3. Application log

Namun tidak terkorelasi dengan log jaringan.

Kondisi Existing

Pada model ini:

1. Log dari firewall, IDS/IPS, router, server, dan aplikasi tidak terpusat
2. Tidak ada korelasi antar-log
3. Deteksi ancaman hanya bergantung pada perangkat masing-masing
4. Investigasi insiden membutuhkan waktu lama karena harus mengakses log satu per satu
5. Tidak ada mekanisme otomatis untuk mengidentifikasi pola serangan kompleks.

Kondisi ini menciptakan blind spot yang signifikan dalam keamanan jaringan.

Arsitektur IBM QRadar SIEM di JOB Tomori

Setelah implementasi IBM QRadar SIEM, JOB Tomori beralih ke arsitektur keamanan modern berbasis log centralization, normalization, dan correlation.

Arsitektur QRadar terdiri dari beberapa komponen utama:

QRadar Console

Merupakan pusat kendali yang menyediakan:

1. Dashboard monitoring
2. Offense management
3. Rule engine
4. Log activity viewer
5. Network activity analysis

Console menjadi titik utama analisis ancaman.

Event Collector

Merupakan pusat kendali yang menyediakan:

1. Firewall
2. IDS/IPS
3. Router
4. Server
5. Aplikasi

Collector memastikan log diterima secara real-time.

Event Processor

Melakukan:

1. Parsing
2. Normalization
3. Correlation
4. Offense generation

Processor adalah inti dari kemampuan deteksi ancaman QRadar.

Log Source Integration

Setiap perangkat keamanan dikonfigurasi untuk mengirim log ke QRadar melalui:

1. Syslog
2. API
3. JDBC
4. WinCollect (untuk Windows Server)

Semua log kemudian dinormalisasi ke dalam format Common Event Format (CEF).

Keunggulan Arsitektur QRadar

Dengan model ini:

1. Semua log terpusat dalam satu platform
2. Korelasi otomatis mendeteksi pola serangan lintas perangkat

3. Offense dihasilkan berdasarkan rule dan analisis perilaku
4. Investigasi insiden menjadi lebih cepat dan akurat
5. Visibilitas jaringan meningkat secara signifikan
6. Tidak ada lagi blind spot antar perangkat

Analisis Data Operasional dan Performa IBM QRadar SIEM

Data operasional QRadar dikumpulkan melalui QRadar Dashboard, Ariel Query Engine, dan Offense Management dalam rentang waktu Januari–Februari 2026 (2 bulan).

Data mencakup:

1. 40 log source yang telah terintegrasi
2. 450 EPS (Event Per Second)
3. 821 offense yang terakumulasi dalam 2 bulan
4. Kategori ancaman: brute force, malware beaconing, unauthorized access, policy violation, dan anomalous behavior.

Availability (Ketersediaan)

Availability diukur berdasarkan:

1. Status service QRadar (ECS, Tomcat, Ariel, Hostcontext)
2. Uptime appliance
3. Ketersediaan log source

Tabel 1 Nilai Rata-rata Availability QRadar JOB Tomori

Metrik	QRadar (Aktual)	Best Practice (HA Cluster)	Keterangan
Mean Availability	99.982%	≥99.99%	Minor downtime saat patching
Min Availability	99.70%	≥99.90%	Terdampak maintenance rutin
Std Deviation	0.214	0.010	Variabilitas karena single-appliance

Analisis

1. Availability QRadar **stabil**, namun sedikit lebih rendah dibanding best practice karena tidak menggunakan HA cluster
2. Variabilitas uptime terjadi saat Ariel indexing dan DSM update
3. Tidak ditemukan service crash selama periode observasi

CPU Utilization

CPU utilization dipengaruhi oleh:

1. Parsing log
2. Correlation rule execution
3. Offense generation
4. Ariel indexing

Tabel 1 Nilai Rata-rata CPU Utilization QRadar

Metrik	QRadar (Aktual)	Keterangan
Average CPU Load	22.4%	Stabil, tidak overload
Median CPU Load	18.1%	Konsisten
Peak CPU	71%	Terjadi saat log burst (shift pagi)

Analisis
1. CPU QRadar tetap dalam batas aman (<80%)
2. Peak CPU terjadi saat offense spike (misalnya brute force burst)
3. Tidak ada indikasi bottleneck atau packet drop

Latency / Response Time (Ariel Query)
Latency diukur dari:
1. Waktu eksekusi query Ariel
2. Waktu load dashboard
3. Waktu offense retrieval

Tabel 2 Nilai Rata-rata Response Time QRadar

Metrik	Nilai	Keterangan
Mean Query Time	2.1 detik	Query ringan
Median Query Time	1.4 detik	Konsisten
Max Query Time	7.8 detik	Query kompleks (join + filter)
Packet Loss	0%	Komunikasi internal stabil

Analisis
1. Response time QRadar **sangat baik** untuk single-appliance
2. Query kompleks membutuhkan waktu lebih lama karena **Ariel indexing** berjalan paralel.

KESIMPULAN

Penelitian ini menunjukkan bahwa penerapan IBM QRadar SIEM memberikan peningkatan signifikan terhadap kemampuan deteksi ancaman keamanan jaringan pada infrastruktur JOB Tomori.

Sebelum implementasi SIEM, sistem monitoring keamanan masih bersifat terfragmentasi, di mana log dari firewall, IDS/IPS, router, server, dan aplikasi tersimpan secara terpisah (siloed). Kondisi ini menyebabkan rendahnya visibilitas jaringan, lambatnya proses investigasi insiden, serta sulitnya mendeteksi pola serangan yang kompleks.

REFERENSI

Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security, 125*, 103028. https://doi.org/10.1016/j.cose.2022.103028

Anggraeni, R., & Maulani, I. E. (2023). Pengaruh teknologi informasi terhadap perkembangan bisnis modern. *Jurnal Sosial Teknologi, 3*(2), 94–98.

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran krusial jaringan komputer dan basis data dalam era digital. *JUSTINFO | Jurnal Sistem Informasi dan Teknologi Informasi, 1*(1), 9–20.

Bezas, K., & Filippidou, F. (2024). Revolutionizing SIEM security: An innovative correlation engine design for multi-layered attack detection. *Sensors, 24*(15), 4901. https://doi.org/10.3390/s24154901

Carrera, B., La Torre, D., & Tavana, M. (2024). A comprehensive investigation of clustering algorithms for user and entity behavior analytics. *Frontiers in Big Data, 7*, 1375818. https://doi.org/10.3389/fdata.2024.1375818

Chic, S. A., & Bilqisthi, M. F. (2024). Tantangan dan peluang blockchain di era digital dalam bidang keamanan data dan transaksi digital. *Journal of Comprehensive Science (JCS), 3*(11).

Fausto, A., Gaggero, G. B., Patrone, F., Girdinio, P., & Marchese, M. (2021). Toward the integration of cyber and physical security monitoring systems for critical infrastructures. *Sensors, 21*(21), 6970. https://doi.org/10.3390/s21216970

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors, 21*(14), 4759. https://doi.org/10.3390/s21144759

Hoshmand, M. O., & Ratnawati, S. (2023). Analisis keamanan infrastruktur teknologi informasi dalam menghadapi ancaman cybersecurity. *Jurnal Sains dan Teknologi, 5*(2), 679–686.

Mohammed, A. S., Reinecke, P., Burnap, P., Rana, O., & Anthi, E. (2022). Cybersecurity challenges in the offshore oil and gas industry: An industrial cyber-physical systems (ICPS) perspective. *ACM Transactions on Cyber-Physical Systems, 6*(3), 1–27. https://doi.org/10.1145/3548691

Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). Integrated security information and event management (SIEM) with intrusion detection system (IDS) for live analysis based on machine learning. *Procedia Computer Science, 217*, 1406–1415. https://doi.org/10.1016/j.procs.2022.12.339

Nabila, A. Z., Yasmine, S., & Stevano, A. (2025). Peran cloud computing terhadap efisiensi infrastruktur dan transformasi jaringan organisasi: Studi literatur. *Jurnal Sains dan Teknologi 4.0, 3*(1), 19–23.

Nandaputra, J., Sukarno, P., & Wardana, A. A. (2024). Detection and prevention system on computer network to handle distributed denial-of-service (DDoS) attack in realtime and multi-agent. *Proceedings of the 2024 10th International Conference on Computer Technology Applications (ICCTA)*, 237–241. https://doi.org/10.1145/3674558.3674592

Prasetia, O., Machfud, S., & Ibnurhus, G. A. (2024). Sosialiasi pengenalan pentingnya cyber security guna menjaga keamanan data di era digital pada siswa/i SMK Bakti Idhata Jakarta. *JIPM: Jurnal Inovasi Pengabdian Masyarakat, 2*(1), 16–20.

Safarzadeh, M., Bagheri, M., Zamani, B., & Shafiei, H. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS ONE, 19*(3), e0299368. https://doi.org/10.1371/journal.pone.0299368

Sani, A., Shabrina, F., Dana, W. P., Hardini, I. R., Juansa, A., Zulfikar, Z., Kumara, I. M. S., Budiasto, J., Rianty, E., & Angin, J. T. K. P. (2025). *Pengantar teknologi informasi: Dampak dan peluang perkembangan teknologi informasi dalam dunia kerja dan bisnis*. Star Digital Publishing.

Stergiopoulos, G., Gritzalis, D. A., & Limnaios, E. (2020). Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns. *IEEE Access, 8*, 128440–128475. https://doi.org/10.1109/ACCESS.2020.3008937

Tommy, S., & Nasution, M. I. P. (2025). Evaluasi manajemen risiko keamanan siber pada infrastruktur digital pemerintah: Studi kasus Pusat Data Nasional (PDN). *Jurnal Manajemen Ekonomi dan Bisnis, 4*(1), 1–26.

Winkler, A. M., Bhattacharya, A., & Bhattacharya, P. (2025). Proactive threat detection in

enterprise systems using Wazuh: A MITRE ATT&CK evaluation. *Computers & Security, 154*, 104460. https://doi.org/10.1016/j.cose.2025.104460

Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection, 34*, 100433. https://doi.org/10.1016/j.ijcip.2021.100433

Yonatan, Y. K., Saepudin, T. H., Siaga, A. P., Arifin, M., Firmansyah, R. N., Daffa, F. M., & Alamsyah, R. (2024). Dampak teknologi lanjutan terhadap keamanan data manajemen sekuriti: Tantangan dan peluang di era digital. *Journal of Engineering Environmental Energy and Science, 3*(2), 59–66.