# ANALISIS KOMPARASI KINERJA IBM QRADAR DAN ELK STACK PADA PT. MAGNUS SEDAYA SELARAS

# SKRIPSI

Diajukan untuk memenuhi salah satu syarat kelulusan Program Sarjana


**KRISTIAN ROSADY**

**11230385**



**Program Studi Sistem Informasi**

**Fakultas Teknik Informasi**

**Universitas Nusa Mandiri**

**Jakarta**


**2024**

# LEMBAR PERSEMBAHAN

***1 Thessalonians 5:16-18***

*[16] Rejoice always, [17] pray continually, [18] give thanks in all circumstances; for this is God's will for you in Christ Jesus.*

Dengan mengucap puji syukur kepada Tuhan Yesus Kristus, Skripsi ini kupersembahkan untuk:

1. Kedua Orang tua tercinta yang telah memberikan motivasi yang besar
2. Dosen Pembimbing Ibu Juarni Siregar, S.Pd.,M.Kom. yang sudah memberikan arahan, tanggapan dan solusi untuk skripsi ini
3. Komunitas Lancaster dan FLSI yang menjadi teman obrolan
4. Rekan SOC dan Staff Magnus yang sudah menyemangati dan memberikan dukungan terhadap skripsi ini

Saya hanya bisa memberikan terimakasih yang besar kepada yang sudah memberikan support untuk pengerjaan skripsi ini semoga diberkati untuk semuanya. Amin.

# LEMBAR PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini,saya:

| | |
|---|---|
| Nama | : Kristian Rosady |
| NIM | : 11230385 |
| Program Studi | : Sistem Informasi |
| Fakultas | : Teknologi Informasi |
| Perguruan Tinggi | : Universitas Nusa Mandiri |

Dengan ini menyatakan bahwa Skripsi yang telah saya buat dengan judul: "Analisis Komparasi Kinerja IBM Qradar Dan ELK Stack Pada PT. Magnus Sedaya Selaras", adalah asli (orisinil) atau tidak plagiat (menjiplak) dan belum pernah diterbitkan/dipublikasikan dimanapun dan dalam bentuk apapun.

Demikianlah surat pernyataan ini saya buat dengan sebenar-benarnya tanpa ada paksaan dari pihak manapun juga. Apabila dikemudian hari ternyata saya memberikan keterangan palsu dan atau ada pihak lain yang mengklaim bahwa Skripsi yang telah saya buat adalah hasil karya milik seseorang atau badan tertentu, saya bersedia diproses baik secara pidana maupun perdata dan kelulusan saya dari Nama Institusi dicabut/dibatalkan.

Dibuat di : Jakarta

Pada tanggal: 7 Januari 2025

Yang menyatakan,


Kristian Rosady

# LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH

Yang bertanda tangan di bawah ini, saya:

| | |
|---|---|
| Nama | : Kristian Rosady |
| NIM | : 11230385 |
| Program Studi | : Sistem Informasi |
| Fakultas | : Teknologi Informasi |
| Perguruan Tinggi | : Universitas Nusa Mandiri |

Dengan ini menyetujui untuk memberikan ijin kepada pihak **Universitas Nusa Mandiri**, Hak Bebas Royalti Non-Eksklusif *(Non-exclusive Royalti-Free Right)* atas karya ilmiah kami yang berjudul: **"Analisis Komparasi Kinerja IBM Qradar dan ELK Stack Pada PT. Magnus Sedaya Selaras"**, beserta perangkat yang diperlukan (apabila ada).

Dengan **Hak Bebas Royalti Non-Eksklusif** ini pihak **Universitas Nusa Mandiri** berhak menyimpan, mengalih-media atau *format*-kan, mengelolaannya dalam pangkalan data *(database)*, mendistribusikannya dan menampilkan atau mempublikasikannya di *internet* atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari kami selama tetap mencantumkan nama kami sebagai penulis/pencipta karya ilmiah tersebut.

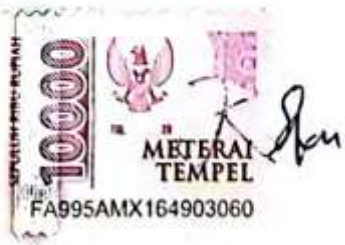
Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak **Universitas Nusa Mandiri**, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya

Dibuat di : Jakarta

Pada tanggal: 7 Januari 2025

Yang menyatakan,




Kristian Rosady

# PERSETUJUAN DAN PENGESAHAN SKRIPSI

Skripsi ini diajukan oleh:

| | |
|---|---|
| Nama | : Kristian Rosady |
| NIM | : 11230385 |
| Program Studi | : Sistem Informasi |
| Fakultas | : Teknologi Informasi |
| Jenjang | : Strata Satu (S1) |
| Judul Skripsi | : Analisis Komparasi Kinerja IBM Qradar Dan ELK Stack Pada PT. Magnus Sedaya Selaras |

Telah dipertahankan pada periode 2024-2 dihadapan penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh Sarjana Komputer (S.Kom) pada Program Sarjana Program Studi Sistem Informasi Fakultas Teknologi Informasi di Universitas Nusa Mandiri.

Jakarta, 06 Februari 2025

**PEMBIMBING SKRIPSI**

Dosen Pembimbing : Juarni Siregar, S.Pd., M.Kom. .....

**DEWAN PENGUJI**

Penguji I : Ani Yoraeni, S.Pd., M.Kom. .....

Penguji II : Ika Kurniawati, M.Kom .....

# LEMBAR PEDOMAN PENGGUNAAN HAK CIPTA

Skripsi yang berjudul **"Analisis Komparasi Kinerja IBM Qradar dan ELK Stack Pada PT. Magnus Sedaya Selaras"** adalah hasil karya tulis asli Kristian Rosady dan bukan hasil terbitan sehingga peredaran karya tulis hanya berlaku di lingkungan akademik saja, serta memiliki hak cipta. Oleh karena itu, dilarang keras untuk menggandakan baik sebagian maupun seluruhnya karya tulis ini, tanpa seizin penulis.

Referensi kepustakaan diperkenankan untuk dicatat tetapi pengutipan atau peringkasan isi tulisan hanya dapat dilakukan dengan seizin penulis dan disertai ketentuan pengutipan secara ilmiah dengan menyebutkan sumbernya.

Untuk keperluan perizinan pada pemilik dapat menghubungi informasi yang tertera di bawah ini:


Nama : Kristian Rosady

Alamat : Jl. H. Taiman Ujung Gg. ZZ No.98 Jakarta Timur

No.Telp : 0821-6517-2043

Mahasiswa E-mail : krosady@gmail.com

# KATA PENGANTAR

Segala syukur dan puji hanya bagi Tuhan Yesus Kristus, oleh karena anugerah-Nya yang melimpah, kemurahan dan kasih setia yang besar sehingga penulis dapat menyelesaikan skripsi dengan lancar tanpa ada suatu kendala apapun. Adapun judul skripsi yang penulis ambil sebagai berikut **"Analisis Komparasi Kinerja IBM Qradar dan ELK Stack Pada PT. Magnus Sedaya Selaras"**

Tujuan penulisan Skripsi ini dibuat sebagai salah satu syarat kelulusan Program Sarjana Universitas Nusa Mandiri. Sebagai bahan penulisan diambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung penulisan ini.

Selama melaksanakan riset dalam menyelesaikan skripsi ini, penulis telah banyak menerima bimbingan, pengarahan, petunjuk dan saran, serta fasilitas yang membantu hingga akhir dari penulisan skripsi ini. Untuk itu penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada yang terhormat:

1. Rektor Universitas Nusa Mandiri
2. Wakil Rektor I Bidang Akademik Universitas Nusa Mandiri
3. Dekan Fakultas Teknologi Informasi Universitas Nusa Mandiri
4. Ketua Program Studi Sistem Informasi Fakultas Teknik dan Informatika Universitas Nusa Mandiri.
5. Ibu Juarni Siregar selaku Dosen Pembimbing Skripsi telah memberikan petunjuk dan pengarahan dalam penyelesaian skripsi.
6. Staff/Karyawan/Dosen di lingkungan Universitas Nusa Mandiri.
7. Manager, Staff dan Rekan SOC di PT. Magnus Sedaya Selaras

Akhirnya penulis berharap semoga Skripsi ini bermanfaat bagi semua pihak yang membantu, meskipun dalam skripsi ini masih banyak kekurangannya. Oleh karena itu kritik dan saran yang membangun tetap penulis harapkan.

Jakarta, 07 Januari 2025

Penulis

Kristian Rosady

# ABSTRAK

Penggunaan komputer di era sekarang menyadari bahwa kenyamanan penggunaan komputer merupakan hal yang paling penting dalam kehidupan sehari-hari mereka. Komputer memainkan peran yang tak tergantikan dan penting dalam penelitian ilmiah, investigasi kriminal, dan banyak lagi. Monitoring adalah tindakan pemantauan yang dapat didefinisikan sebagai kesadaran terhadap informasi yang ingin diketahui. Kejahatan Siber (*Cybercrime*) merupakan tantangan serius bagi masyarakat dan berbahaya bagi individu atau organisasi yang menjadi korban Tujuan ini Melakukan analisis terhadap implementasi *network forensics* menggunakan tools IBM Qradar SIEM dan ELK Stack guna mendeteksi ancaman serangan siber serta analisis perbandingan dalam mencari kinerja yang lebih baik IBM Qradar adalah sebuah rangkaian solusi yang menyediakan intelijen ancaman dan wawasan yang lebih baik terhadap serangan siber ELK Stack adalah solusi sumber terbuka yang kuat dan banyak digunakan untuk manajemen log, analisis data, dan visualisasi. Solusi ini terdiri dari tiga komponen inti: *Elasticsearch, Logstash,* dan *Kibana*, yang secara kolektif dikenal sebagai ELK Stack. Dimulai dengan Elasticsearch, dan berkembang dengan Logstash dan Kibana Pada Analisa yang dilakukan di on-site, *Personal Computer Security Operations Center* digunakan untuk menjalankan *system* IBM Qradar dan ELK Stack dalam mendeteksi serangan siber Penelitian ini menggunakan 8 (delapan) tahapan *network forensics, Preparation, Detection, Incident Response, Collection, Preservation, Examination, Investigation,* dan *Presentation* sebagai acuan untuk komparasi tools. Hasil dari komparasi tersebut menunjukkan bahwa IBM QRadar lebih efektif dalam konfigurasi *rules*, *response tools*, pengumpulan paket data serangan, serta *friendly UI* dan visualisasi data.

**Kata Kunci: Komputer, Monitoring, IBM Qradar, ELK Stack, *Network Forensics***

# ABSTRACT

*Today's computer users realize that the convenience of using a computer is the most important thing in their daily lives. Computers play an irreplaceable and important role in scientific research, criminal investigations, and more. Monitoring is the act of monitoring which can be defined as the awareness of information that one wants to know. Cybercrime is a serious challenge to society and is harmful to individuals or organizations that are victims of it This objective Conducts an analysis of the implementation of network forensics using IBM Qradar SIEM and ELK Stack tools to detect cyber attack threats and a comparative analysis in search of better performance IBM Qradar is a suite of solutions that provides threat intelligence and better insight into cyber attacks. ELK Stack is a powerful and widely used open-source solution for log management, data analysis, and visualization. The solution consists of three core components: Elasticsearch, Logstash, and Kibana, collectively known as the ELK Stack. Starting with Elasticsearch, and expanding with Logstash and Kibana In the analysis conducted on-site, the Personal Computer Security Operations Center was used to run the IBM Qradar system and ELK Stack in detecting cyber attacks This research uses 8 (eight) stages of network forensics, Preparation, Detection, Incident Response, Collection, Preservation, Examination, Investigation, and Presentation as a reference for tool comparison. The results of the comparison show that IBM QRadar is more effective in configuring rules, response tools, collecting attack data packages, as well as friendly UI and data visualization.*



***Keywords: Computer, Monitoring, IBM Qradar, ELK Stack, Network Forensics***

# DAFTAR PUSTAKA


[1] Zen Munawar and Novianti Indah Putri , “KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA”, j-sika, vol. 2, no. 01, pp. 14–20, Jul. 2020.

[2] Sari, N., & Cahyani, D. (2022). Perancangan Sistem Informasi Monitoring Sertifikat Menggunakan Extreme Programming. Jurnal Ilmiah Computer Science, 1(1), 1-6.

[3] Fitri Nova, Pratama, M. D., & Prayama, D . (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. JITSI : Jurnal Ilmiah Teknologi Sistem Informasi, 3(1), 1–7.

[4] R. Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya," *Technology and Economics Law Journal,* vol. 2, no. 2, p. 2, 2023.

[5] Hanafi, Motivasi dan Jenis Serangan Dasar Cyber Security dan Forensic, Sleman: Deepublish, 2022.

[6] M. A. Kothekar, Building a Next-Gen SOC with IBM QRadar, Birmingham: Packt Publishing, 2022.

[7] IBM Security White Paper, “Sense and detect modern threats with the most sophisticated security analytics platform,” March 2019, https: //www.ibm.com/downloads/cas/G6E26E3J. Diakses : 29 November 2024.

[8] User Guide IBM 7.4.3 Ariel Query Language Guide. IBM. https://www.ibm.com/docs/en/SS42VS_7.4/pdf/b_qradar_aql.pdf. Diakses: 6 Des 2024

[9] G, Peter “PostgreSQL 15 Cookbook: 100+ expert solutions across scalability, performance optimization, essential commands, cloud provisioning, backup, and recovery” India: GitforGits, 2023.

[10] Patel, Ram “Securing Networks with ELK Stack: Building zero trust network defense”, Cetakan Pertama, Noida: BPB Publications, 2024. pp. 173-174.

[11] S. Fleming, DevOps and Site Reliability Engineering (SRE) Handbook: Non Programmer's Guide, England: Amazon Digital Services LLC, 2020.

[12] A. Srivastava, Elasticsearch 8 for Developers: A beginner's guide to indexing, analyzing, searching, and aggregating data, India: BPB Publications, 2023. pp. 38 - 139.

[13] Sabharwal, Navin and Ravinshankar Shukla “Application Observability with Elastic: Real-time metrics, logs, errors, traces, root cause analysis, and anomaly detection”, Cetakan Pertama. BPB Publications: India 2022

[14] Suskalo, D., Moric, Z., Redzepagic , J., & Regvart, D. "Comparative Analysis of IBM Qradar and Wazuh for Security Information and Event Management," in DAAAM Proceedings, Vienna, 2023.

[15] W. Christoper and R. Zulfargian, "Pemantauan dan Pengawasan Serangan Siber SSH Brute Force di Indonesia dengan IBM QRadar Community Edition," *Jurnal Ilmiah Teknik Informatika (TEKINFO),* 2024.

[16] F. Frattini, U. Giordano and V. Conti, "Facing Cyber-Physical Security Threats by PSIM-SIEM Integration," 2019 15th European Dependable Computing Conference (EDCC), Naples, Italy, 2019, pp. 83-88

[17] Khan, M. A., Azim, A., Abazari , F., Eargle, F., & Gardiner, J, "Automated offense Prioritization for SIEM using Probabilistic Machine Learning Models," in Proceedings of the Canadian Conference on Artificial Intelligence, Ontario, 2024.

[18] L. Harris, "AI in Cloud Security Operations : Streaming Incident Response," Stanford University, 2024.

[19] R. Botwright, ed Team Operations: Black Box Hacking, Social Engineering & Web App Scanning, United Kingdom and Ireland: Pastor Publishing Ltd, 2023.

[20] Diogenes, Yuri and Dr. Erdal Ozkaya, Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, United Kingdom: Packt Publishing Ltd., 2019.