Implementasi SIEM Menggunakan Elastic Sebagai Sistem Monitoring Keamanan Server Infrastruktur Di PT Lintasarta

Imola Anggraini
2103421029

PROGRAM STUDI BROADBAND MULTIMEDIA
JURUSAN TEKNIK ELEKTRO
POLITEKNIK NEGERI JAKARTA
2025

Implementasi SIEM Menggunakan Elastic Sebagai Sistem Monitoring Keamanan Server Infrastruktur Di PT Lintasarta

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Terapan

Imola Anggraini

2103421029

PROGRAM STUDI BROADBAND MULTIMEDIA

JURUSAN TEKNIK ELEKTRO

POLITEKNIK NEGERI JAKARTA

2025

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya saya sendiri dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Imola Anggraini

NIM : 2103421029

Tanda Tangan :

Tanggal : 26 Juni 2025

LEMBAR PENGESAHAN

SKRIPSI

Tugas Akhir diajukan oleh :

Nama : Imola Anggraini

NIM : 2193421029

Program Studi : Broadband Multimedia

Judul Tugas Akhir : Implementasi SIEM Menggunakan Elastic Sebagai Sistem Monitoring Keamanan Server Infrastruktur Di PT Lintasarta

Telah diuji oleh tim penguji dalam Sidang Tugas Akhir pada (Isi Hari dan Tanggal) dan dinyatakan LULUS.

Pembimbing I : Dandun Widhiantoro A.Md.,M.T ( )

NIP. 197011251995031001

Pembimbing II : Darwin Prasetya Eka Gunawan ( )

NIP. 87131151

Depok, Juli 2025

Disahkan oleh

Ketua Jurusan Teknik Elektro

Dr. Murie Dwiyaniti, S.T.,M.T

NIP. 197803312003122002

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat, karunia, dan kekuatan-Nya, sehingga penulis dapat menyelesaikan Skripsi ini dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Terapan pada program studi yang penulis tempuh, Broadband Multimedia.

Perjalanan dalam menyelesaikan Skripsi ini bukanlah hal yang mudah. Ada banyak proses panjang yang harus dilalui mulai dari kebingungan awal, jatuh bangun dalam mengolah data, hingga akhirnya dapat merangkai semua menjadi sebuah Skripsi ini. Namun, di balik setiap tantangan, selalu ada tangan-tangan baik yang hadir memberi semangat, bantuan, dan doa. Oleh karena itu, penulis mengucapkan terima kasih kepada :

1. Dandun Widhiantoro A.,Md.,M.T, selaku dosen pembimbing yang telah dengan sabar dan penuh perhatian membimbing penulis selama proses penyusunan Tugas Akhir ini. Bimbingan Bapak bukan hanya sebatas arahan akademik, tetapi juga menjadi penyemangat saat semangat penulis mulai meredup. Terima kasih atas setiap waktu yang diluangkan, setiap revisi yang diperiksa dengan teliti, serta setiap nasihat yang begitu berarti. Semoga Allah membalas segala ketulusan dan dedikasi Bapak dalam mendidik kami, para mahasiswa, yang masih terus belajar menjadi dewasa.
2. Darwin Prasetya Eka Gunawan, S.I, yang telah membantu penulis dalam memperoleh data dan informasi yang sangat diperlukan dalam penelitian ini. Bantuan dan kerja samanya sangat berarti, tidak hanya secara teknis, tetapi juga menjadi bentuk nyata dari kepercayaan dan dukungan yang mendorong penulis untuk terus melangkah maju. Terima kasih atas kesediaannya untuk membantu tanpa pamrih, meski di tengah kesibukan yang luar biasa.
3. Bundaku tercinta, Ibu Sari Novia Inda, yang doanya adalah pelindung paling kuat, dan cintanya adalah alasan utama penulis untuk tidak menyerah. Ibu adalah alasan di balik setiap perjuangan ini. Terima kasih atas pelukan yang selalu menenangkan, semangat yang tak pernah padam, dan pengorbanan yang tak terucap kata. Tanpa Ibu, semua ini tak mungkin terwujud. Tugas akhir ini

adalah bentuk kecil dari rasa terima kasih penulis yang tak akan pernah cukup diungkapkan hanya dengan kata.

4. Sahabat-sahabat terkasih, yang selalu hadir menjadi tempat berbagi tawa di tengah tekanan, dan menjadi bahu saat air mata tak terbendung. Terima kasih atas setiap dukungan, motivasi, dan kebersamaan yang membuat perjalanan ini terasa lebih ringan dan penuh warna. Kalian bukan hanya teman seperjuangan, tapi keluarga yang dipilih oleh hati.

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Tugas Akhir ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 26 Juni 2025

Imola Anggraini

Implementasi SIEM Menggunakan Elastic Sebagai Sistem Monitoring Keamanan Server Infrastruktur Di PT Lintasarta

Abstrak

Keamanan infrastruktur server menjadi aspek penting dalam menjaga kestabilan operasional perusahaan, khususnya bagi perusahaan berbasis teknologi informasi seperti PT Lintasarta. Salah satu upaya penting dalam menjaga keamanan tersebut adalah dengan memantau aktivitas sistem secara real-time dan mendeteksi ancaman sejak dini. Penelitian ini bertujuan untuk membangun dan mengimplementasikan sistem SIEM (Security Information and Event Management) berbasis Elastic Stack, yang terdiri dari komponen Filebeat, Winlogbeat, Metricbeat, Elasticsearch, Kibana, serta tambahan ElastAlert sebagai sistem notifikasi otomatis. Sistem ini dirancang untuk mencatat log aktivitas login user dan performa server dari sistem operasi Windows maupun Linux, serta menampilkan data tersebut dalam bentuk visualisasi yang interaktif melalui dashboard Kibana. Selain itu, sistem juga mampu memberikan peringatan otomatis kepada administrator jika terdeteksi aktivitas mencurigakan seperti login gagal berulang atau penggunaan sumber daya yang tinggi.
Hasil pengujian menunjukkan bahwa sistem dapat mencatat log dengan akurat, menampilkan informasi metrik server secara real-time, dan mengirim notifikasi alert secara otomatis. Dengan demikian, implementasi SIEM berbasis Elastic Stack terbukti efektif dalam meningkatkan visibilitas dan keamanan infrastruktur server perusahaan. Sistem ini juga bersifat open-source dan fleksibel untuk dikembangkan lebih lanjut sesuai kebutuhan organisasi.

Kata Kunci: SIEM, Elastic Stack, Kibana

SIEM Implementation Using Elastic as an Infrastructure Server Security Monitoring System at PT Lintasarta

Abstract

Server infrastructure security is a crucial aspect in maintaining the stability of company operations, especially for information technology-based companies such as PT Lintasarta. One of the important efforts in maintaining such security is by monitoring system activity in real-time and detecting threats early on. This research aims to build and implement an Elastic Stack-based SIEM (Security Information and Event Management) system, which consists of Filebeat, Winlogbeat, Metricbeat, Elasticsearch, Kibana, and ElastAlert as an automatic notification system. The system is designed to log user login activity and server performance from Windows and Linux operating systems, and display the data in the form of interactive visualizations through the Kibana dashboard. In addition, the system is also able to provide automatic alerts to administrators if suspicious activity is detected such as repeated failed logins or high resource usage.
The test results show that the system can record logs accurately, display real-time server metric information, and send alert notifications automatically. Thus, the implementation of Elastic Stack-based SIEM has proven effective in improving the visibility and security of the company's server infrastructure. The system is also open-source and flexible to be further developed according to the needs of the organization.

Keywords: SIEM, Elastic Stack, Kibana

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Server merupakan suatu sistem komputer besar yang terintegrasi dan tersusun pada suatu jaringan komputer besar yang menyediakan suatu layanan bagi para pengguna yang biasa disebut sebagai *client*. Suatu server umumnya telah menjalankan banyak proses untuk membantu dalam memenuhi permintaan dari *client*. Oleh sebab itu, sering sekali server mengalami beberapa kendala yang disebabkan karena tidak adanya sumber daya (*resource*) yang mumpuni atau sesuai untuk memenuhi *resource* perbaikan server Hal tersebut dapat menyebabkan layanan atau *service server* mati secara mendadak dikarenakan file *system kernel* memutuskan untuk mematikan layanan pada server yang membutuhkan *resource* yang sangat besar. File *system kernel* adalah komponen inti atau penting dari suatu sistem operasi. *Kernel* memiliki tanggung jawab untuk menyelesaikan tugas-tugas tingkat rendah/bawah seperti untuk manajemen storage, manajemen CPU dan manajemen memori.

Untuk menghindari terjadinya kebocoran informasi, Perusahaan maupun organisasi perlu menerapkan langkah-langkah pengamanan yang efektif. Beberapa diantaranya meliputi penerapan enkripsi pada data, penguatan sistem akses terhadap informasi sensitif, serta memastikan bahwa seluruh karyawan memiliki pemahaman dan pelatihan yang memadai terkait pentingnya menjaga kerahasiaan data. Di sisi lain, individu juga berperan penting dalam menjaga keamanan informasi dengan cara menggunakan teknologi yang aman, seperti membuat kata sandi yang kuat dan tidak sembarangan membagikan data pribadi. Upaya pencegahan kebocoran informasi dapat dilakukan melalui tindakan preventif yang mengacu pada standar keamanan informasi yang berlaku.

SIEM adalah sistem yang dapat digunakan untuk mengelola log yang dihasilkan dari berbagai sumber data seperti *endpoint*, perangkat jaringan, maupun *firewall* namun untuk kasus serangan siber umumnya data log didapatkan dari IDS *(Intrusion Detection System)*. IDS merupakan perangkat keras/lunak yang digunakan sebagai sensor untuk monitoring dan mendeteksi adanya intrusi pada lalu lintas jaringan. Elasticsearch adalah aplikasi open source dibuat menggunakan

bahasa pemrograman *Java* yang berfungsi sebagai alat pencarian, penyimpanan dan analisis log, dibangun berdasarkan konsep kerja sistem pencarian *Apache Lucene*.

Dalam era digital, keamanan infrastruktur server merupakan aspek yang sangat penting untuk menjaga keberlangsungan operasional Perusahaan Lintasarta, sebagai penyedia layanan ICT, penerapan SIEM sangat membantu dalam menganalisa log dengan mengumpulkan semua informasi yang mengakses server yang sedang berjalan.

Masalah dengan menjalankan server dalam jumlah besar tanpa sistem pemantauan server adalah sulitnya untuk memantau penggunaan sumber daya server secara *real time* untuk gangguan seperti *disk* penuh dan kinerja CPU (*Central Processing Unit*)itu melampaui apa yang seharusnya ditindaklanjuti untuk pengobatan sesegera mungkin (Sulasno & Saleh, 2020).

Pada skripsi ini bertujuan untuk membuat log data dari *agent* di server agar bisa diterapkan pada sistem monitoring server dengan memanfaatkan aplikasi Elastic guna merekam data log dari server yang akan di monitoring dan memberikan notifikasi otomatis kepada pengguna. Selain itu, sistem ini juga dirancang untuk mengetahui kondisi data log server secara *real-time*, sehingga dapat meningkatkan keamanan dan efisiensi dalam pemantauan infrastruktur server.

1.2 Perumusan Masalah

Pengelolaan dan pemantauan yang efektif atas server infrastruktur sangat penting, untuk menjaga keberlanjutan dan keamanan system. Tantangannya adalah:

1. Bagaimana cara mengimplementasikan sistem SIEM berbasis Elastic Stack yang mampu mengumpulkan data log dari berbagai sumber server secara real-time?
2. Bagaimana sistem dapat mencatat dan memantau aktivitas login user secara akurat, baik login yang berhasil maupun yang gagal?
3. Bagaimana sistem dapat menampilkan informasi performa server seperti CPU, memori, dan disk secara real-time dalam bentuk visualisasi yang informatif?
4. Bagaimana cara mengintegrasikan fitur notifikasi otomatis menggunakan ElastAlert untuk mendeteksi aktivitas mencurigakan atau penggunaan sumber daya berlebih?

5. Bagaimana sistem SIEM dapat meningkatkan visibilitas dan keamanan infrastruktur server secara efektif dan efisien?

1.3 Tujuan

1. Mengimplementasikan sistem SIEM berbasis Elastic Stack untuk mengumpulkan data log dari server Windows dan Linux secara real-time.
2. Mencatat dan memantau aktivitas login user secara akurat, serta menampilkan status login melalui dashboard.
3. Menyediakan visualisasi performa server secara real-time, termasuk penggunaan CPU, memori, dan disk.
4. Mengintegrasikan ElastAlert untuk memberikan notifikasi otomatis terhadap aktivitas mencurigakan atau penggunaan sumber daya yang melebihi ambang batas.
5. Meningkatkan visibilitas dan keamanan infrastruktur server perusahaan melalui sistem monitoring yang responsif dan terintegrasi.

Batasan dari penelitian yaitu ini hanya berfokus pada sistem monitoring aktivitas user untuk mengetahui berapa dan status user dalam proses mengakses suatu server internal. Dan juga untuk memonitoring kapasitas dari beberapa komponen server berupa CPU, *Memory* dan *Disk* secara *real time*. Aplikasi Elastic ini merupakan aplikasi yang dapat memvisualisasikan log *event* ke dalam sebuah dashboard monitoring atau yang disebut dengan Kibana.

5.1 Luaran

Dari skripsi ini diharapkan membuat data log dari agent di server agar bisa ditampilkan dengan benar di dashboard yang akan dibuat, dan pada dashboard juga bisa memonitoring data yang interaktif, memungkinkan visual data log secara *real-time*, aktivitas login, serta insiden keamanan dari keterangan user yang mempunyai keterangan "*failed login*".

a. Luaran Wajib

1) Laporan Tugas Akhir

2) Luaran Tambahan

1) Artikel Ilmiah dengan judul "Perbandingan SIEM dan SOAR : Pilar Utama Keamanan Informasi Modern

BAB V
SIMPULAN

Berdasarkan hasil implementasi dan pengujian sistem Security Information and Event Management (SIEM) berbasis Elastic Stack yang telah dilakukan, maka dapat disimpulkan beberapa hal sebagai berikut :

1. Sistem SIEM berhasil diimplementasikan dengan baik menggunakan komponen Elastic Stack, yang terdiri dari Filebeat, Winlogbeat, Metricbeat, Elasticsearch, dan Kibana. Sistem ini mampu mengumpulkan data log dari berbagai sumber server baik berbasis Windows maupun Linux secara real-time.
2. Sistem mampu melakukan pencatatan dan pemantauan aktivitas login user secara akurat, baik login yang berhasil maupun yang gagal. Informasi log yang terkumpul dapat divisualisasikan melalui dashboard Kibana, sehingga memudahkan administrator dalam menganalisis aktivitas pengguna dan mendeteksi potensi ancaman keamanan seperti upaya login mencurigakan.
3. Monitoring performa server dapat dilakukan secara menyeluruh dan real-time, mencakup penggunaan CPU, memori, dan disk. Visualisasi data metrik melalui Kibana memberikan gambaran menyeluruh terhadap kondisi infrastruktur server dan memungkinkan tindakan preventif ketika sumber daya mendekati batas kritis.
4. Integrasi ElastAlert berhasil menambahkan fitur alert otomatis, di mana sistem dapat mengirimkan notifikasi melalui email kepada administrator jika terdeteksi pola aktivitas yang mencurigakan atau penggunaan sumber daya yang melebihi ambang batas yang telah ditentukan. Fitur ini sangat bermanfaat dalam meningkatkan kecepatan respons terhadap insiden keamanan.
5. Secara keseluruhan, sistem SIEM berbasis Elastic Stack yang dikembangkan terbukti efektif dan efisien dalam mendukung kegiatan monitoring keamanan server. Sistem ini dapat meningkatkan visibilitas terhadap aktivitas jaringan dan memberikan perlindungan proaktif terhadap potensi ancaman siber, sehingga sangat relevan untuk diterapkan di lingkungan perusahaan seperti PT Lintasarta.

DAFTAR PUSTAKA

Admi, A., & Maulana, A. N. (2020). Penerapan Elastic Stack sebagai Tools Alternatif Pemantauan Traffic Jaringan dan Host pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia. *Jurnal Sistem dan Teknologi Informasi Indonesia*.

Alfiansyah, F., & Murad, Skom., Mkom, F. A. (2020). Implementasi Security Information And Event Management (Siem) Pada Lingkungan Itsec Asia Menggunakan Elastic Siem.

Anggara, T. R. (2023). Strategi Implementasi Siem Untuk Mengurangi Risiko Terhadap Kebocoran Informasi. *Jurnal Teknologi Terpadu*.

Bayu, P. K. (2022). Implementasi Server Log Monitoring System menggunakan Elastic Stack. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* , 1814-1824.

Ehis, A.-m. T. (2023). Optimization of Security Information and Event Management (SIEM) Infrastructures, and Events Correlation/Regression Analysis for Optimal Cyber Security Posture. *Archive of Advanced Engineering Sains*, 1-10.

Hadi, M. S., & Putri, D. A. (2024). Implementasi Security Information And Event Management (Siem) Untuk Deteksi Dan Analisa Insiden Keamanan Pada Web Server.

Hafiz, M., & Soewito, B. (2022). Information Security Systems Design Using SIEM, SOAR and Honeypot. *Jurnal Pendidikan Tambusai*, Halaman 15527-15541.

Heluka, H. D., & Sulisyto, W. (2023). Perancangan Dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server. *Jurnal Ilmiah Komputer*, 912-922.

Lintasarta. (11 de Desember de 2020). *Perbedaan SIEM dan SOAR dalam Keamanan Siber*. Fonte: Lintasarta: https://www.lintasarta.net/blog/solution/it-services/security-it-services/perbedaan-siem-dan-soar-dalam-keamanan-siber/

Nugraha, F., Khalimi, T., & Herwanto, H. (2025). Implementasi Security Information dan Event Management (SIEM) Pada Sistem Akademik Universitas Kuningan. *JURNAL BUFFER INFORMATIKA*.

Paw, M. P., Aspriyono, H., & Al Akbar, A. (2024). Implementation Of Security Information And Event Management (Siem) In Monitoring Networks At SMA 1 Muhammadiyah Boarding School. *Media Computer Science*.

Putra, P. H. (2020). Implementasi Log Management Server Menggunakan Elk (Elastic Search, Logstash Dan Kibana) Stack Pada Server Web Snort Di PT.XYZ . *Research Gate*.

Putra, W. P., Burjulius, R., Al Hilmi, M. A., & Samarudin. (2024). Implementasi Sistem Manajemen Log untuk Penanggulangan Serangan Server dengan SIEM. *IKRAITH-INFORMATIKA V*.

Rahman, D., Amnur, H., & Rahmayuni, I. (2020). Monitoring Server dengan Prometheus dan Grafana serta Notifikasi Telegram. *Jurnal Ilmiah Teknologi Sistem Informasi*, 133-138.

Ramli, M., & Soewito, B. (2023). Monitoring dan Evaluasi Keamanan Jaringan dengan Pendekatan Security Information and Security Management (SIEM). *Factor Exacta*.

Rasyidi, B., & Pratama, F. (2024). Sistem Monitoring Server di PT. XYZ Media Indonesia Berbasis Grafana dan Prometheus. *Indonesian Journal of Machine Learning and Computer Science*, 1456-1465.

Rizal, K., Supriyandi, Zen, M., & Eka, M. (2022). Perancangan Server Kantor Desa Tomuan Holbung Berbasis Client Server. *Bulletin of Information Technology (BIT)*, 27-33.

Sholihah, W., Pripambudi, S., & Mardiyono, A. (2020). Log Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack). *Jurnal Teknologi Informasi dan Multimedia*, 12-20.

Sholihah, W., Pripambudi, S., & Mardiyono, A. (2020). og Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack). *JTIM : Jurnal Teknologi Informasi dan Multimedia*, 12-20.

DAFTAR RIWAYAT HIDUP

Imola Anggraini

Lahir di Jakarta, 21 Oktober 2002. Bertempat tinggal di Jakarta Selatan, dengan memulai Pendidikan SD nya di SDN Ragunan 05 Pagi dari tahun 2008-2014 Dilanjut dengan Pendidikan menengah pertama di SMPN 7 Pekanbaru hingga tahun 2017 Setelah itu berlanjut kependidikan menengah atas di SMA Negeri 6 Pekanbaru. Penulis melanjutkan Pendidikan tinggi di Politeknik Negeri Jakarta.