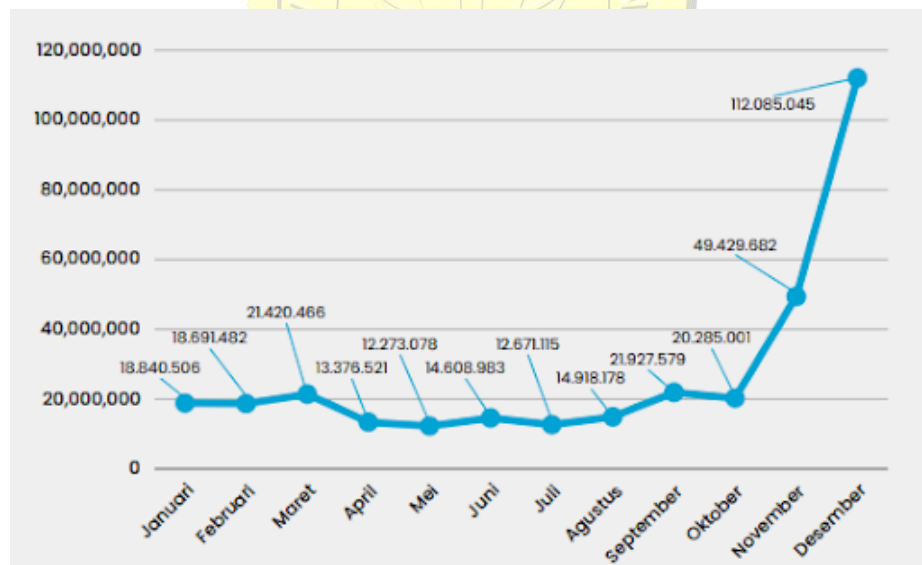


BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam beberapa tahun terakhir, ruang siber Indonesia menunjukkan peningkatan ancaman yang signifikan. Berdasarkan laporan Lanskap Keamanan Siber Indonesia 2024 oleh Badan Siber dan Sandi Negara (BSSN), tercatat sebanyak 330 juta trafik anomali siber sepanjang tahun 2024 dengan jenis ancaman tertinggi berupa *Mirai Botnet* yang menargetkan perangkat *Internet of Things* (IoT). Selain itu, terdapat 514.508 aktivitas *ransomware*, 26 juta aktivitas *phishing*, serta 241 dugaan insiden kebocoran data dengan lebih dari 56 juta data terekspos di *darknet*, yang sebagian besar menimpa sektor pemerintahan (Badan Siber dan Sandi Negara, 2024).



Gambar I-1 Data Lanskap Keamanan Siber Indonesia 2024
(Sumber: Badan Siber dan Sandi Negara (2024, hlm. 30), diakses melalui <https://alika.pesisirbaratkab.go.id/files/272/E-BOOK/262/Lanskap-Keamanan-Siber-Indonesia-2024--BSSN.pdf>)

Fakta ini menunjukkan bahwa tingkat ancaman siber di Indonesia meningkat secara drastis dan belum sepenuhnya diimbangi dengan kesiapan infrastruktur keamanan yang memadai. BSSN juga menegaskan bahwa percepatan transformasi digital di sektor publik belum disertai dengan penguatan postur keamanan siber yang optimal, terutama di tingkat instansi kecil dan daerah (Badan Siber dan Sandi Negara, 2024). Kondisi ini mengindikasikan perlunya solusi keamanan yang efisien, adaptif, dan mudah diimplementasikan oleh berbagai institusi.

Sebagai respons terhadap meningkatnya ancaman siber dan keterbatasan infrastruktur keamanan, beberapa penelitian telah mengembangkan sistem *Security Information and Event Management* (SIEM) sebagai salah satu solusi untuk mendeteksi dan merespons ancaman siber secara terpusat. Salah satu penelitian tersebut dilakukan oleh Sijabat & Evo (2023) yang menunjukkan bahwa penerapan SIEM berbasis *Elastic Stack* mampu mendeteksi berbagai jenis serangan pada situs web sesuai kategori *OWASP Top 10*, serta membantu administrator mempercepat proses identifikasi dan tindak lanjut terhadap insiden keamanan. Namun, mereka juga menekankan bahwa penerapan SIEM memerlukan sumber daya dan biaya yang cukup besar, kondisi tersebut menunjukkan adanya kebutuhan terhadap solusi yang lebih ringan dan efisien untuk lingkungan dengan sumber daya terbatas.

Sementara itu, penelitian oleh Nugraha et al. (2025) menyoroti tantangan implementasi SIEM dalam sistem akademik Universitas Kuningan. Sistem yang dikembangkan terbukti meningkatkan efektivitas deteksi ancaman dan efisiensi manajemen insiden, penelitian tersebut juga menemukan bahwa penerapan SIEM masih menghadapi kendala teknis berupa kompleksitas konfigurasi aturan deteksi

dan kebutuhan infrastruktur yang besar untuk memproses data log dalam jumlah masif. Hal ini menunjukkan bahwa solusi SIEM konvensional belum sepenuhnya cocok untuk diterapkan di lingkungan dengan sumber daya terbatas.

Selain aspek kapabilitas deteksi ancaman, beberapa penelitian terbaru juga menekankan pentingnya evaluasi performa sistem SIEM. Manzoor et al. (2024) menemukan bahwa *platform* SIEM *open-source* seperti Wazuh, Elastic Security, OSSIM, dan SIEMonster menunjukkan perbedaan signifikan dalam *throughput* pemrosesan log (*Event per Second*) dan konsumsi sumber daya (CPU dan memori) ketika log volume meningkat. Evaluasi ini menunjukkan bahwa performa pemrosesan log merupakan faktor krusial dalam efektivitas SIEM, terutama pada lingkungan dengan keterbatasan sumber daya. Penelitian performa yang dibahas sebagian besar berfokus pada platform berskala besar, sementara evaluasi kinerja SIEM ringan atau modular untuk skenario *low-resource* masih jarang dibahas.

Dari penelitian tersebut dapat diidentifikasi adanya celah yaitu SIEM *open-source* yang ada seperti Wazuh, OSSIM, SIEMonster dan Elasticsearch, Loki, Kibana (ELK) Stack efektif dalam deteksi ancaman, tetapi masih relatif memakan *resource* dan kompleks untuk diterapkan di organisasi kecil atau laboratorium dengan keterbatasan sumber daya. Selain itu, solusi yang sudah ada seperti Splunk, Microsoft Sentinel, IBM QRadar, dan sejenisnya, lebih menekankan integrasi enterprise, bukan efisiensi. Selain itu, penelitian yang secara spesifik melakukan evaluasi performa SIEM pada lingkungan dengan keterbatasan sumber daya berdasarkan indikator terukur seperti penggunaan CPU, memori, *throughput* pemrosesan log, *latency*, dan penggunaan storage masih terbatas.

Meskipun berbagai penelitian menunjukkan bahwa SIEM *open-source* maupun enterprise efektif dalam mendukung deteksi dan respons insiden keamanan, solusi SIEM konvensional masih memiliki keterbatasan berupa kompleksitas implementasi, biaya pengelolaan, serta kebutuhan sumber daya komputasi yang besar. Penelitian sebelumnya juga cenderung berfokus pada peningkatan kapabilitas deteksi ancaman dan implementasi pada infrastruktur yang memadai, sehingga kajian mengenai efektivitas SIEM pada lingkungan *low-resource* masih terbatas. Selain itu, masih sedikit penelitian yang mengukur efisiensi penggunaan *resource* seperti CPU, memori, *throughput*, dan *latency*, serta menguji tingkat akurasi pendekatan *rule-based* pada arsitektur SIEM. Dengan demikian, terdapat research gap berupa masih terbatasnya solusi SIEM *lightweight* yang dirancang untuk lingkungan dengan sumber daya terbatas namun tetap memiliki kemampuan monitoring dan deteksi ancaman yang memadai. Oleh karena itu, Xemarify diposisikan sebagai alternatif SIEM *lightweight* untuk memenuhi kebutuhan monitoring keamanan pada perangkat atau server dengan sumber daya terbatas.

Untuk menjawab permasalahan tersebut, penelitian ini berfokus pada pengembangan Xemarify, yaitu aplikasi SIEM *lightweight* yang dibangun menggunakan Golang pada komponen *agent* dan *manager*, PostgreSQL, serta Svelte+kit sebagai *frontend*. Solusi ini diharapkan menghasilkan SIEM yang efisien dalam konsumsi sumber daya, mudah dikembangkan, dan dapat menjadi alternatif solusi monitoring keamanan untuk lingkungan berskala kecil maupun menengah.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang dan membangun Xemarify sebagai sistem SIEM *lightweight* berbasis *web* yang mampu melakukan pengumpulan, analisis, dan visualisasi *log* secara efisien pada lingkungan dengan sumber daya terbatas?
2. Bagaimana efisiensi penggunaan sumber daya serta tingkat akurasi *rule-based detection* dalam mendeteksi aktivitas anomali atau ancaman keamanan secara *real-time* pada lingkungan *low-resource*?
3. Bagaimana hasil kinerja Xemarify dalam pengujian menggunakan *framework* ISO/IEC 25010 di lingkungan yang memiliki keterbatasan sumber daya?

1.3 Batasan Masalah

1. Penelitian ini berfokus pada pengembangan Xemarify sebagai sistem SIEM *lightweight* yang terdiri atas komponen utama, yaitu *collector*, *analyzer*, *storage*, dan *dashboard web*.
2. Xemarify memproses log berbasis *syslog* atau *JSON* dari *server* Linux dan aplikasi web sederhana. Integrasi dengan perangkat jaringan, *IDS/IPS*, sensor industri, serta dukungan sistem operasi selain Linux tidak dibahas.
3. Fungsi sistem dibatasi pada pengumpulan, normalisasi, korelasi dan agregasi log, analisis berbasis aturan, serta visualisasi melalui dashboard web. Fitur lanjutan seperti *machine learning*, *threat intelligence*, dan SOAR tidak termasuk dalam penelitian.

4. Implementasi dilakukan pada lingkungan *local* dan pengujian dilakukan pada lingkungan *cloud* dengan spesifikasi sumber daya terbatas. Pengujian pada infrastruktur skala *enterprise* tidak termasuk dalam ruang lingkup penelitian ini.
5. Evaluasi menggunakan ISO/IEC 25010:2023 dengan fokus pada karakteristik *Performance Efficiency* dan *Security*. Subkarakteristik *resistance* serta karakteristik lain di luar kedua aspek tersebut tidak diuji.
6. Wazuh digunakan sebagai sistem pembandingan hanya pada aspek performa yang relevan. Penelitian tidak membandingkan keseluruhan kapabilitas Xemarify dan Wazuh serta tidak membahas aspek organisasi, manajemen risiko, hukum, maupun regulasi keamanan siber.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dikemukakan, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang dan membangun Xemarify sebagai sistem SIEM *lightweight* berbasis Golang dengan arsitektur *Manager* dan *Agent* untuk lingkungan dengan sumber daya terbatas.
2. Mengukur efisiensi penggunaan sumber daya serta akurasi *rule-based detection* Xemarify dalam mendeteksi aktivitas anomali secara *real-time*.
3. Mengevaluasi Xemarify berdasarkan karakteristik *Performance Efficiency* dan *Security* pada ISO/IEC 25010:2023, dengan Wazuh sebagai pembandingan pada aspek performa.

1.5 Manfaat Penelitian

1.5.1 Manfaat bagi Penulis

1. Memberikan kontribusi terhadap pengembangan ilmu di bidang keamanan informasi, khususnya dalam kajian *Security Information and Event Management*.
2. Mengembangkan keterampilan dalam merancang arsitektur dan desain sistem yang modular.
3. Menambah literatur akademik mengenai penerapan *rule-based correlation* sederhana untuk deteksi ancaman keamanan berbasis *log* pada lingkungan bersumber daya terbatas.

1.5.2 Manfaat bagi Pengguna

1. Membantu proses monitoring keamanan dengan penggunaan sumber daya yang lebih efisien.
2. Menyediakan alternatif solusi bagi instansi pendidikan, organisasi kecil dalam SIEM dengan keterbatasan infrastruktur
3. Menjadi dasar pengembangan *ecosystem open-source* yang dapat digunakan secara mandiri untuk meningkatkan kesadaran dan kemampuan keamanan siber di lingkungan akademik maupun pemerintahan daerah.