

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan proses perancangan, implementasi, dan pengujian Xemarify, diperoleh kesimpulan sebagai berikut:

1. Xemarify berhasil dirancang dan dibangun sebagai aplikasi Security Information and Event Management (SIEM) *lightweight* berbasis web dengan arsitektur modular yang terdiri atas *Agent* dan *Manager*. Sistem mampu menjalankan fungsi utama SIEM, yaitu pengumpulan log, pemrosesan *event*, deteksi berbasis rule, pengelolaan *alert*, *audit log*, serta visualisasi informasi keamanan secara terpusat pada lingkungan dengan sumber daya terbatas.
2. Xemarify menunjukkan penggunaan sumber daya yang lebih efisien dibandingkan Wazuh pada lingkungan pengujian, baik dari sisi CPU maupun memori. Sistem juga mampu memproses beban hingga 3.000 EPS secara stabil pada konfigurasi 2 vCPU dan RAM 4 GB. Pada pengujian *rule-based detection*, Xemarify memperoleh *Precision* 100,00%, *Recall* 50,00%, *Accuracy* 66,67%, dan *F1-score* 66,67%. Hasil tersebut menunjukkan bahwa sistem mampu menghasilkan *alert* yang tepat, namun masih memerlukan penyempurnaan pada pembentukan *event* untuk mengurangi *false negative*.
3. Berdasarkan evaluasi karakteristik *Performance Efficiency* dan *Security* ISO/IEC 25010:2023, Xemarify mampu mempertahankan fungsi monitoring keamanan pada lingkungan *low-resource*. Dari aspek performa, sistem menunjukkan throughput yang stabil dengan latency yang masih terkendali

hingga batas operasionalnya. Dari aspek keamanan, implementasi autentikasi JWT, RBAC, validasi *agent*, dan *audit log* meningkatkan kemampuan monitoring, integritas pencatatan, serta akuntabilitas aktivitas pengguna. Dengan demikian, Xemarify memenuhi tujuan penelitian sebagai SIEM *lightweight* yang mendukung *monitoring* keamanan pada lingkungan dengan keterbatasan sumber daya.

Secara keseluruhan, Xemarify telah memenuhi tujuan penelitian sebagai aplikasi SIEM *lightweight* yang menyediakan fungsi dasar pengumpulan, deteksi, pencatatan, dan visualisasi aktivitas keamanan. Xemarify memiliki efisiensi penggunaan sumber daya yang baik pada konfigurasi pengujian, tetapi masih memerlukan penyempurnaan pada rantai pembentukan event, kemampuan deteksi, kapasitas beban tinggi, dan beberapa fungsi lanjutan SIEM.

5.2 Saran

Berdasarkan hasil dan keterbatasan penelitian, saran untuk pengembangan dan penelitian selanjutnya adalah:

1. Mengoptimalkan mekanisme ingestion Xemarify melalui *batching*, *asynchronous processing*, *backpressure*, dan pengaturan *worker* untuk meningkatkan kapasitas pemrosesan pada beban tinggi.
2. Memperbaiki pembentukan dan pengiriman event dari aplikasi maupun Agent, serta menambahkan pengujian integrasi otomatis agar dapat mengurangi *false negative* pada proses *rule-based detection*.

3. Memperluas pengujian dengan variasi skenario serangan, sumber log, durasi, dan jumlah pengulangan yang lebih besar sehingga evaluasi *Accuracy*, *Precision*, *Recall*, dan *F1-score* lebih representatif.
4. Mengembangkan fitur keamanan dan SIEM, seperti penguatan audit log, rotasi Agent secret, retensi log yang dapat dikonfigurasi, serta penambahan *compliance reporting*, *vulnerability scanning*, dan *integrasi threat intelligence*.
5. Melakukan evaluasi pada infrastruktur dan skala organisasi yang lebih beragam, serta menggunakan konfigurasi perangkat keras dan protokol *ingest* yang setara agar perbandingan dengan SIEM lain lebih objektif.
6. Penelitian selanjutnya dapat mengembangkan Xemarify untuk organisasi yang memiliki keterbatasan sumber daya IT dan anggaran infrastruktur, seperti sekolah, instansi pemerintah berskala kecil, laboratorium pendidikan, atau organisasi kecil dan menengah.

Penelitian selanjutnya disarankan melakukan pengujian pada infrastruktur yang lebih beragam dan dalam skala yang lebih besar. Perbandingan dengan SIEM lain juga perlu menggunakan protokol *ingest*, bentuk payload, durasi, serta spesifikasi perangkat keras yang setara agar hasil perbandingan kinerja dapat dilakukan secara lebih sebanding.