

HALAMAN MOTTO

“Jika kamu jatuh ke dalam arus, jangan biarkan dirimu terbawa oleh arus, dan jangan pula melawan arus.”



HALAMAN PERSEMBAHAN

Puji syukur penulis panjatkan ke hadirat Allah SWT atas rahmat, kesehatan, dan kesempatan yang diKarunia-Nya sehingga skripsi ini dapat terselesaikan dengan baik. Skripsi ini penulis persembahkan kepada pihak-pihak yang telah memberikan dukungan dan bantuan selama proses penyusunan. Penulis mengucapkan terima kasih kepada:

1. Rektor Universitas Putra Bangsa, atas kesempatan dan fasilitas yang diberikan sehingga penulis dapat menyelesaikan studi di institusi ini.
2. Ketua Program Studi Ilmu Komputer, atas arahan, bimbingan, serta dukungan yang diberikan selama penulis menempuh pendidikan.
3. Ibu Lolanda Hamim Annisa, S.Kom., M.Kom., selaku dosen pembimbing, atas bimbingan, kesabaran, waktu, serta ilmu yang telah diberikan kepada penulis.
4. Seluruh dosen dan staf Universitas Putra Bangsa, atas ilmu dan pelayanan selama proses akademik.
5. Kedua orang tua tercinta, yang selalu memberikan doa, kasih sayang, dukungan moral maupun material, serta kepercayaan yang menjadi sumber kekuatan bagi penulis hingga dapat menyelesaikan pendidikan dan skripsi ini.
6. Tidak lupa rekan seperjuangan penulis yang selalu *Consistent, Innovative*, dan *Adaptive*, yang menjadi teman berdiskusi, berbagi ide, serta saling memberikan semangat menghadapi berbagai tantangan selama perkuliahan dan penyusunan skripsi.

ABSTRAK

Peningkatan kebutuhan pemantauan keamanan mendorong penggunaan *Security Information and Event Management* (SIEM), namun sebagian besar *platform* SIEM memiliki kompleksitas implementasi serta kebutuhan memori dan sumber daya yang relatif tinggi sehingga kurang sesuai diterapkan pada lingkungan *low-resource*. Penelitian ini bertujuan merancang dan membangun Xemarify sebagai aplikasi SIEM *lightweight* untuk mendukung aktivitas *Security Operation Center*, serta mengevaluasi efisiensi sumber daya, akurasi *rule-based detection*, dan kapabilitas keamanan sistem. Xemarify mendukung pengumpulan, normalisasi, analisis *event*, pembentukan *alert* dan *audit log*, serta visualisasi melalui *dashboard* web. Penelitian menggunakan metode *Research and Development* dengan pengujian eksperimental pada lingkungan 2 vCPU dan RAM 4 GB. Evaluasi mengacu pada karakteristik *Performance Efficiency* dan *Security* ISO/IEC 25010:2023 melalui pengujian *overhead*, kapasitas EPS, utilisasi sumber daya, *throughput*, *breaking point*, serta analisis keamanan *As-Is* dan *To-Be*. Hasil pengujian menunjukkan bahwa *manager* Xemarify mencatat rata-rata CPU 1,22% dan memori 8,37 MB, sedangkan *manager* Wazuh mencapai 28,03% CPU dan 318,52 MB memori pada skenario *overhead* yang sama. Pada sisi *agent*, Xemarify hanya memerlukan 11,04 MB memori dibandingkan Wazuh sebesar 63 MB. Sistem tetap stabil hingga 3.000 EPS dan mencapai *breaking point* pada 5.000 EPS. Pengujian deteksi menghasilkan *accuracy* 66,67%, *recall* 50%, *precision* 100%, dan *F1-score* 66,67%. Penerapan JWT, RBAC, autentikasi *agent*, validasi *event*, dan *audit log* meningkatkan kapabilitas keamanan pada mekanisme *monitoring*. Hasil tersebut menunjukkan bahwa Xemarify merupakan alternatif SIEM *lightweight* yang menekankan efisiensi sumber daya untuk fungsi *security monitoring* dasar pada lingkungan *low-resource*.

Kata Kunci: *Security Information and Event Management, lightweight, ISO/IEC 25010:2023, rule-based detection, Security Operation Center*

ABSTRACT

The growing demand for security monitoring has increased the adoption of Security Information and Event Management (SIEM) platforms. However, most SIEM solutions involve high implementation complexity and require substantial memory and computing resources, making them less suitable for low-resource environments. This research aims to design and develop Xemarify, a lightweight SIEM application that supports Security Operation Center (SOC) activities while evaluating resource efficiency, rule-based detection accuracy, and system security capabilities. Xemarify provides log collection, normalization, event analysis, alert and audit log generation, and visualization through a web-based dashboard. This study employed the Research and Development (R&D) method with experimental testing on an environment consisting of 2 vCPUs and 4 GB RAM. The evaluation followed the Performance Efficiency and Security characteristics of ISO/IEC 25010:2023, including overhead testing, EPS capacity, resource utilization, throughput, breaking-point testing, and As-Is and To-Be security analysis. The results show that the Xemarify manager recorded an average CPU utilization of 1.22% and memory consumption of 8.37 MB, whereas the Wazuh manager reached 28.03% CPU utilization and 318.52 MB memory under the same overhead scenario. On the agent side, Xemarify required only 11.04 MB of memory compared to 63 MB for Wazuh. The system remained stable up to 3,000 EPS and reached its breaking point at 5,000 EPS. Detection testing achieved 66.67% accuracy, 50% recall, 100% precision, and an F1-score of 66.67%. The implementation of JWT, RBAC, agent authentication, event validation, and audit logging enhanced the security capabilities of the monitoring mechanism. These findings demonstrate that Xemarify is a viable lightweight SIEM alternative that emphasizes resource efficiency for fundamental security monitoring in low-resource environments.

Keywords: *Security Information and Event Management, lightweight, ISO/IEC 25010:2023, rule-based detection, Security Operation Center*

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah Swt. atas segala rahmat, karunia, dan pertolongan-Nya sehingga penulis dapat menyelesaikan skripsi berjudul **“Rancang Bangun Xemarify: Aplikasi *Security Information and Event Management Lightweight* untuk Mendukung *Security Operation Center*”** sebagai salah satu syarat memperoleh gelar Sarjana Komputer. Skripsi ini membahas perancangan dan pembangunan Xemarify sebagai aplikasi SIEM untuk lingkungan dengan sumber daya terbatas:

1. Allah Swt. atas kesehatan, kekuatan, kemudahan, dan kesempatan selama proses penyusunan skripsi.
2. Ibu Lolanda Hamim Annisa, S.Kom., M.Kom., selaku dosen pembimbing, atas waktu dan arahan selama penyusunan skripsi.
3. Seluruh dosen dan tenaga kependidikan Universitas Putra Bangsa atas ilmu dan pelayanan selama masa perkuliahan.
4. Kedua orang tua dan keluarga penulis yang senantiasa memberikan doa, dukungan, motivasi, serta bantuan selama penulis menempuh pendidikan.
5. Teman, rekan yang selalu *Consistent, Innovative*, dan *Adaptive*, serta pihak yang telah memberikan dukungan dalam penelitian dan penyusunan skripsi .

Penulis berharap penelitian ini dapat memberikan manfaat bagi *pengembangan sistem*, khususnya aplikasi SIEM yang ringan dan dapat digunakan pada lingkungan *low-resource*. Selain itu, penelitian ini diharapkan dapat menjadi referensi bagi mahasiswa, peneliti, maupun pengembang yang akan melakukan penelitian lebih lanjut dalam bidang keamanan informasi dan *Security Operation Center*.

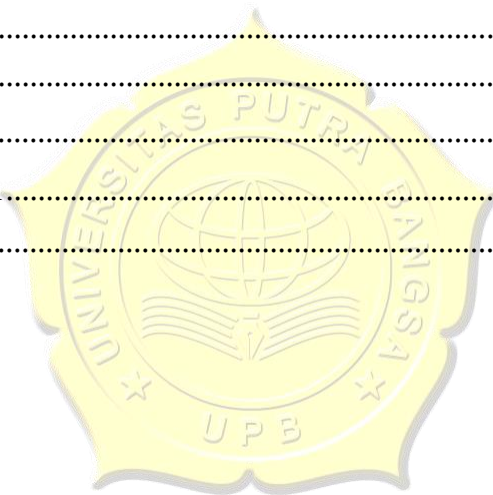
DAFTAR ISI

HALAMAN SAMPUL DEPAN	i
HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN UJIAN SKRIPSI	iv
HALAMAN PERNYATAAN BEBAS PLAGIARISME	v
HALAMAN MOTTO	vi
HALAMAN PERSEMBAHAN	vii
ABSTRAK	viii
KATA PENGANTAR.....	x
DAFTAR ISI	xi
DAFTAR TABEL	xv
DAFTAR GAMBAR	xvii
DAFTAR LAMPIRAN	xix
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	5
1.3 Batasan Masalah.....	5
1.4 Tujuan Penelitian.....	6
1.5 Manfaat Penelitian.....	7
1.5.1 Manfaat bagi Penulis.....	7
1.5.2 Manfaat bagi Pengguna.....	7
BAB II	
KAJIAN PUSTAKA	8
2.1 Tinjauan Teori	8
2.1.1 Rancang Bangun	8
2.1.2 Aplikasi <i>Security</i>	9
2.1.3 ISO/IEC 25010.....	9
2.1.4 Cara Ukur <i>Framework</i> ISO/IEC 25010	11
2.1.5 Keamanan Informasi	11
2.1.6 <i>Logging</i> dan <i>Monitoring</i>	12

2.1.7	<i>Security Operation Center (SOC)</i>	13
2.1.8	<i>Security Information Management (SIM)</i>	13
2.1.9	<i>Security Event Management (SEM)</i>	14
2.1.10	Komponen dan Arsitektur SIEM	14
2.1.11	Wazuh.....	17
2.1.12	<i>Lightweight</i>	18
2.1.13	Golang.....	19
2.1.14	PostgreSQL	20
2.1.15	Svelte dan SvelteKit.....	21
2.2	Penelitian Terdahulu	22
2.3	Kerangka Penelitian	27
2.4	Keaslian Penelitian.....	27
BAB III METODOLOGI PENELITIAN		30
3.1	Tahapan Penelitian	30
3.1.1	Observasi Data	31
3.1.2	Analisis Permasalahan	31
3.1.3	Rumusan Masalah.....	31
3.1.4	Kajian Literatur.....	32
3.1.5	Analisis Kebutuhan Solusi.....	32
3.1.6	Solusi yang Diusulkan	32
3.1.7	Implementasi Sistem	33
3.1.8	Pengujian dan Evaluasi	33
3.1.9	Hasil Pengujian	34
3.2	Objek dan Subjek Penelitian	34
3.3	Metode Penelitian.....	35
3.4	Metode Pengumpulan Data	36
3.4.1	Observasi Sistem.....	36
3.4.2	Pengukuran Kinerja.....	37
3.4.3	Pengujian Fungsional Keamanan.....	37
3.5	Metode Perancangan Sistem	37
3.5.1	Analisis Kebutuhan Sistem	37

3.5.2 Perancangan Model Konseptual Sistem.....	40
3.5.3 Perancangan UML	41
3.6 Alat dan Bahan.....	46
3.7 Prosedur Pengujian.....	46
3.7.1 Karakteristik Kualitas pada ISO 25010:2023	47
3.7.2 Karakteristik Kualitas yang Digunakan dalam Penelitian	48
3.7.3 Definisi Operasional dan Kriteria <i>Lightweight</i>	51
3.7.4 Indikator Keberhasilan Sistem	52
3.7.5 Metode Pengujian Berbasis Skoring Fungsional	53
3.7.6 Pelaksanaan Pengujian <i>Performance Efficiency</i>	55
3.7.7 Pelaksanaan Pengujian <i>Security</i>	56
BAB IV HASIL DAN PEMBAHASAN	57
4.1 Lingkungan dan Konfigurasi Pengujian.....	57
4.1.1 Objek Pengujian Website	57
4.1.2 Topologi dan Skenario Pengujian	59
4.1.3 Perangkat Lunak yang Dipakai	60
4.2 Skenario dan Alur Pengujian.....	61
4.2.1 Alur Pelaksanaan Pengujian.....	61
4.2.2 Skema Pelaksanaan Pengujian	63
4.2.3 Dasar Pemilihan Variabel Pengujian <i>Performance Efficiency</i>	63
4.2.4 Dasar Evaluasi Karakteristik <i>Security</i>	66
4.2.5 Penetapan Kondisi <i>As-Is</i> dan <i>To-Be</i>	71
4.2.6 Teknik Pengumpulan Data dan Analisis Data <i>Security</i>	72
4.2.7 Skenario Pengujian <i>Detection Rate Rule-Based Detection</i>	76
4.2.8 Skenario Pengujian Skoring Fungsional Berbobot	81
4.3 Implementasi dan Hasil	88
4.3.1 Tampilan Antarmuka Sistem	88
4.3.2 Implementasi <i>Rule Engine</i>	91
4.4 Hasil Pengujian Sistem.....	95
4.4.1 <i>Performance Efficiency</i>	95
4.4.2 <i>Security</i>	102

4.4.3	Tingkat Akurasi Deteksi <i>Rule Based Detection</i>	125
4.4.4	Skoring Fungsional Berbobot (Manzoor et al.)	131
4.5	Pembahasan.....	134
4.5.1	Xemarify sebagai SIEM <i>Lightweight</i>	135
4.5.2	Pembahasan <i>Performance Efficiency</i>	136
4.5.3	Pembahasan Tingkat Akurasi Deteksi <i>Rule Engine</i>	139
4.5.4	Pembahasan Security kondisi <i>As-is</i> dan <i>To-be</i>	141
4.5.5	Pembahasan Kelengkapan Fungsional (J. Manzoor)	144
4.5.6	Implikasi Penelitian.....	145
4.5.7	Keterbatasan Penelitian.....	146
4.5.8	Rekomendasi.....	147
BAB V PENUTUP.....		150
5.1	Kesimpulan.....	150
5.2	Saran.....	151
DAFTAR PUSTAKA.....		153
LAMPIRAN.....		158



DAFTAR TABEL

Tabel II-1 Penelitian Terdahulu.....	22
Tabel II-2 Keaslian Penelitian.....	27
Tabel III-1 Karakteristik Kualitas Produk ISO/IEC 25010:2023	47
Tabel III-2 Karakteristik dan Subkarakteristik <i>Performance Efficiency</i> dan <i>Security</i>	50
Tabel III-3 Indikator Keberhasilan Sistem.....	52
Tabel III-4 Operasionalisasi Evaluasi Karakteristik <i>Performance Efficiency</i> Berdasarkan ISO/IEC 25010:2023	55
Tabel III-5 Operasionalisasi Evaluasi Karakteristik <i>Security</i> Berdasarkan ISO/IEC 25010:2023.....	56
Tabel IV-1 Lingkungan Pengujian	57
Tabel IV-2 Perangkat Lunak Yang Digunakan.....	60
Tabel IV-3 Justifikasi Variable <i>Performance Efficiency</i>	64
Tabel IV-4 Kriteria Perbandingan <i>Security</i> pada Kondisi <i>As-Is</i> dan <i>To-Be</i>	68
Tabel IV-5 Format Analisis <i>As-is</i> dan <i>To-be</i>	76
Tabel IV-6 Skenario Pengujian Tingkat Akurasi Deteksi	77
Tabel IV-7 Klasifikasi Hasil <i>Uji Detection Rate</i>	79
Tabel IV-8 Fitur Skoring Fungsional Berbobot Xemarify	82
Tabel IV-9 Kriteria Nilai Metode J. Manzoor.....	85
Tabel IV-10 Lembar Pengujian Skoring Fungsional Berbobot.....	86
Tabel IV-11 Struktur Data Alert pada Xemarify	94
Tabel IV-12 Hasil Pengujian <i>VU Overhead Test</i>	95
Tabel IV-13 Hasil Pengujian <i>EPS Capacity Test</i> Xemarify	96
Tabel IV-14 Hasil Pengujian <i>EPS Capacity Test</i> Wazuh.....	97
Tabel IV-15 Hasil Pengujian <i>Resource Utilization - Overhead Agent</i>	98
Tabel IV-16 Hasil Pengujian <i>Resource Utilization - EPS Capacity</i>	98
Tabel IV-17 Hasil Pengujian <i>Capacity - Throughput</i>	99
Tabel IV-18 Hasil Pengujian <i>Capacity - Breaking Point Test</i>	100
Tabel IV-19 Hasil Pengujian <i>Capacity - Narrowdown Test</i>	100
Tabel IV-20 Hasil Perbandingan <i>As-is To-be Confidentiality</i>	108
Tabel IV-21 Hasil Perbandingan <i>As-is To-be Integrity</i>	111
Tabel IV-22 Hasil Perbandingan <i>As-is To-be Non-Repudiation</i>	115
Tabel IV-23 Hasil Perbandingan <i>As-is To-be Accountability</i>	119
Tabel IV-24 Hasil Perbandingan <i>As-is To-be Authenticity</i>	122
Tabel IV-25 Hasil Rekapitulasi Pengujian <i>Security</i>	122
Tabel IV-26 Hasil Pengujian Tingkat Deteksi Xemarify	126
Tabel IV-27 Detail Hasil Setiap Percobaan.....	126
Tabel IV-28 Hasil Rekapitulasi Pengujian Tingkat Deteksi.....	127

Tabel IV-29 Hasil Perhitungan <i>Detection Rate</i>	127
Tabel IV-30 Hasil Skoring Fungsional Xemarify	131



DAFTAR GAMBAR

Gambar I - 1 Data Lanskap Keamanan Siber Indonesia 2024	1
Gambar II-1 Kerangka Pemikiran.....	27
Gambar III-1 Tahapan Penelitian Xemarify	30
Gambar III-2 Model Konseptual Sistem.....	40
Gambar III-3 <i>Usecase Diagram</i>	41
Gambar III-4 <i>Flowchart Login</i>	41
Gambar III-5 <i>Flowchart User Management</i>	42
Gambar III-6 <i>Flowchart Rule Management</i>	42
Gambar III-7 <i>Dataflow Diagram</i> (level0).....	43
Gambar III-8 Activity Diagram Sistem Login Sebelum di <i>Install</i> Xemarify	43
Gambar III-9 Activity Diagram Sistem <i>Login</i> Setelah di <i>Install</i> Xemarify	44
Gambar III-10 Activity Diagram Sistem Login Sebelum Di <i>Install</i> Xemarify (Performance).....	44
Gambar III-11 Activity Diagram Sistem <i>Login</i> Sebelum Di <i>Install</i> Xemarify (Performance)	45
Gambar III-12 <i>Entity Relationship Diagram</i>	45
Gambar IV-1 Tampilan Halaman Setup	88
Gambar IV-2 Tampilan Halaman Login.....	88
Gambar IV-3 Tampilan Halaman Dashboard	88
Gambar IV-4 Tampilan Halaman Users	89
Gambar IV-5 Tampilan Halaman Events	89
Gambar IV-6 Tampilan Halaman Alerts.....	89
Gambar IV-7 Tampilan Halaman Audit Logs	89
Gambar IV-8 Tampilan Halaman Rules	90
Gambar IV-9 Tampilan Halaman Agents	90
Gambar IV-10 Tampilan Halaman Enrollment Token	90
Gambar IV-11 Halaman Agent Onboarding (Docs).....	90
Gambar IV-12 Arsitektur <i>Rule Engine</i>	91
Gambar IV-13 Hasil Pengecekan <i>Ownership</i> access.log dan error.log.....	102
Gambar IV-14 Hasil Pengecekan Hak Akses User Lain.....	103
Gambar IV-15 Hasil Pencatatan Log Nginx	104
Gambar IV-16 Hasil Implementasi Perlindungan Data Log Xemarify Menggunakan <i>JWT Middleware</i>	105
Gambar IV-17 Hasil Implementasi <i>Role</i> yang Diizinkan	106
Gambar IV-18 Hasil Pengujian Runtime Hak Akses Setiap Role Terhadap Endpoint.....	107
Gambar IV-19 Hasil Implementasi Pemeriksaan <i>Event</i> dari <i>Agent</i> oleh <i>Middleware X-Agent-Secret</i>	109

Gambar IV-20 Hasil Implementasi Validasi <i>Payload Events</i>	110
Gambar IV-21 Hasil Pengujian <i>Runtime</i> Validasi Data dari Agent.....	110
Gambar IV-22 Hasil Implementasi <i>Audit Log</i>	111
Gambar IV-23 Hasil Implementasi Skema Database Audit Log	113
Gambar IV-24 Hasil Implementasi Pencatatan Log (Kasus Login).....	113
Gambar IV-25 Hasil Implementasi Pencatatan Log Ketika <i>Manager/Analyst</i> Melakukan <i>Update Status Alerts</i>	114
Gambar IV-26 Hasil Pengujian <i>Runtime</i> Pencatatan <i>Audit Log</i>	115
Gambar IV-27 Hasil Pengujian Pencarian Log secara Manual.....	116
Gambar IV-28 Hasil Implementasi Pencarian Log Berdasarkan Tindakan	117
Gambar IV-29 Hasil Implementasi Fitur Filter Log berdasarkan Aksi, Waktu Dan Kata Kunci	118
Gambar IV-30 Pembentukan <i>access token JWT</i> pada Xamarify	120
Gambar IV-31 Hasil Implementasi Pemeriksaan <i>agent secret</i> pada <i>middleware</i>	121
Gambar IV-32 Hasil Implementasi Pencocokan <i>Agent</i> dengan <i>Secret Key</i>	121



DAFTAR LAMPIRAN

Lampiran 1 Kartu Bimbingan	159
Lampiran 2 Kehadiran Seminar Proposal	160
Lampiran 3 Arsitektur Antar Komponen	161
Lampiran 4 Arsitektur Rule Engine	162
Lampiran 5 Alur Pemrosesan Event	163
Lampiran 6 Source Code.....	164

