

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERNYATAAN ORISINALITAS	ii
LEMBAR PERNYATAAN ORISINALITAS	iii
LEMBAR PERNYATAAN ORISINALITAS	iv
ABSTRAK.....	v
ABSTRACT.....	vi
KATA PENGANTAR	vii
UCAPAN TERIMA KASIH	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL.....	xiv
DAFTAR SINGKATAN	xv
BAB 1 USULAN GAGASAN.....	1
1.1 Deskripsi Umum Masalah.....	1
1.2 Analisis Masalah.....	3
1.2.1 Aspek Teknologi.....	3
1.2.2 Aspek Regulasi dan Hukum.....	4
1.2.3 Aspek Bisnis dan Sosial.....	5
1.3 Analisis Solusi yang Ada	6
1.4 Tujuan Tugas Akhir	6
1.5 Batasan Tugas Akhir	7
1.6 Metodologi.....	7
BAB 2 TINJAUAN PUSTAKA	9
2.1 <i>Cyberattack</i>	9
2.1.1 Probe Attack.....	9

2.1.2	User to Root Attack (U2R)	11
2.1.3	Remote to User Attack (R2L)	11
2.1.4	DoS dan DDoS.....	12
2.2	<i>Cybersecurity</i>	12
2.2.1	<i>Intrusion Prevention System (IPS)</i>	12
2.2.2	<i>Machine Learning</i>	13
2.2.3	<i>Security Information and Event Management</i>	17
BAB 3	SPESIFIKASI DAN DESAIN SISTEM.....	19
3.1	Spesifikasi Sistem	19
3.2	Desain Sistem.....	22
3.3	Metode Pengukuran yang Sesuai dengan Solusi Terpilih.....	27
3.1.1	<i>IPS Snort</i>	27
3.1.2	<i>Machine Learning</i>	29
3.1.3	Security Information and Event Management (SIEM)	31
BAB 4	IMPLEMENTASI.....	32
4.1	Deskripsi Umum Implementasi	32
4.2	Detail Implementasi	34
4.3	Prosedur Pengoperasian Solusi	48
BAB 5	PENGUJIAN.....	50
5.1	Skema Pengujian Sistem.....	50
5.1.1	Batasan Pengujian Sistem	50
5.1.2	Kategori Pengujian Sistem.....	52
5.2	Proses Pengujian dan Analisis Hasil.....	54
5.2.1	Pengujian Snort tanpa Machine Learning.....	54
5.2.2	Pengujian Model Machine Learning pada Google Colab.....	57
5.2.3	Pengujian dan Analisis Kinerja Model pada Real System.....	62
5.2.4	Hasil Pengujian Wazuh SIEM	80

5.3	Rangkuman Hasil Pengujian.....	81
BAB 6 KESIMPULAN DAN SARAN		84
6.1	Kesimpulan	84
6.2	Saran	85
DAFTAR PUSTAKA		86
LAMPIRAN.....		92