

DAFTAR ISI

ABSTRAK	i
ABSTRACT.....	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	v
DAFTAR GAMBAR	vii
DAFTAR TABEL.....	x
DAFTAR SIMBOL.....	xi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Tujuan.....	4
1.4 Batasan Masalah.....	4
1.5 Metodologi Penelitian.....	4
1.5.1 Identifikasi dan Perumusan Masalah	5
1.5.2 Menentukan Tujuan	6
1.5.3 Pengembangan Sistem	6
1.5.4 Kesimpulan dan Saran.....	8
1.6 Sistematika Penulisan.....	8
BAB 2 TINJAUAN PUSTAKA	10
2.1 Struktur Organisasi.....	10
2.2 Landasan Teori	17
2.2.1 Cybercrime	17
2.2.2 Security Operation Center (SOC)	23
2.2.3 Security Information and Event Management (SIEM)	26
2.2.4 Security Event	31
2.2.5 Wazuh	32
BAB 3 ANALISIS DAN PERANCANGAN SISTEM	35

3.1	Identify	35
3.1.1	Kondisi Saat Ini.....	35
3.1.2	Prosedur yang berjalan.....	40
3.2	Assess	42
3.2.1	Analisis Masalah	42
3.2.2	Analisis Serangan.....	43
3.2.3	Analisis Solusi.....	51
3.2.4	Analisis Requiremnet	54
3.2.5	Analisis Kebutuhan Hardware	55
3.2.6	Analisis Kebutuhan Software.....	55
3.2.7	Analisis Pengguna.....	55
3.2.8	Perancangan model SOC.....	57
3.2.9	Perancangan arsitketur sistem	63
3.2.10	Perancangan Prosedur	88
3.2.11	Perancangan Pengujian	90
BAB 4	IMPLEMENTASI DAN PENGUJIAN	92
4.1	Protect.....	92
4.1.1	Perangkat yang Digunakan	92
4.1.2	Implementasi Sistem SIEM	94
4.2	Monitor	126
4.2.1	Pengujian.....	126
BAB 5	Kesimpulan dan Saran	136
5.1	Kesimpulan.....	136
5.2	Saran	136
	Daftar Pustaka	138