

DAFTAR ISI

HALAMAN SAMPUL	i
LEMBAR PENGESAHAN	ii
PERNYATAAN KEASLIAN PENELITIAN	iii
KATA PENGANTAR	iv
DAFTAR ISI.....	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL.....	xi
INTISARI.....	xii
<i>ABSTRACT</i>	xiii
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Tujuan Penelitian.....	2
1.4. Batasan Masalah.....	3
1.5. Manfaat Penelitian.....	3
1.6. Metode Penelitian.....	3
1.7. Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1. Tinjauan Pustaka	5
2.2. Dasar Teori	11
2.2.1 Virtual Private Server.....	11
2.2.2 Docker Container	12
2.2.3 Elastic Stack.....	12
2.2.4 Beat	13
2.2.5 Elasticsearch.....	13
2.2.6 Kibana	14
2.2.7 Wazuh	14
2.2.8 Nginx.....	15
2.2.9 Elastalert.....	16
2.2.10 Chrome.....	17
2.2.11 Termius	17

2.2.12	Brute Force	18
2.2.13	Web Application Attack.....	19
BAB III BAHAN DAN METODE PENELITIAN.....		21
3.1.	Waktu dan Tempat	21
3.2.	Alat Penelitian	21
3.3.	Bahan Penelitian.....	22
3.4.	Tahapan Penelitian	25
3.5.	Perancangan dan Pengembangan Sistem	26
3.5.1	Perancangan Topologi SOC.....	26
3.5.2	Perancangan <i>Dashboards</i> SOC	27
3.5.3	Instalasi SOC.....	29
3.5.4	Perancangan Alert SOC	32
3.5.5	Konfigurasi Alert SOC.....	33
3.5.6	Dokumentasi Monthly Report SOC	36
3.6.	Tahap Pengujian	37
BAB IV HASIL DAN PEMBAHASAN		39
4.1.	Analisis <i>log</i> Serangan Menuju <i>Dashboards</i> SOC	39
4.2.	Pengiriman notifikasi terhadap serangan.....	51
4.3.	Hasil Pengamatan Serangan Selama 3 Bulan.....	55
BAB V PENUTUP.....		57
5.1.	Kesimpulan.....	57
5.2.	Saran	57
DAFTAR PUSTAKA		58
LAMPIRAN.....		60