



DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PENGESAHAN	iii
PERNYATAAN BEBAS PLAGIASI	iv
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xiii
INTISARI	xiv
ABSTRACT.....	xv
BAB I.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian.....	3
1.6 Sistematika Penulisan.....	3
BAB II.....	4
2.1 Analisis Log <i>Domain Name System</i> (DNS)	4
2.2 Pemanfaatan Data Log Sebagai <i>Log Event Management</i>	4
2.3 Landasan Teori	10
2.3.1 Log DNS <i>Server</i>	10
2.3.2 <i>Data Enrichment</i>	11
2.3.3 <i>Monitoring</i>	11
2.3.4 Memcached.....	11
2.3.5 Elasticsearch Logstash Kibana (ELK Stack).....	12
2.3 Hipotesis.....	14
BAB III	15
3.1 Alat dan Bahan	15
3.1.1 Perangkat Keras	15
3.1.2 Perangkat Lunak	15
3.2.1 Arsitektur Sistem Keseluruhan	16
3.2.2 Arsitektur Sistem pada Fokus Penelitian	17
3.2.3 Alur Penelitian	18
3.2.4 Metode Pengumpulan dan Penguraian Data Log <i>Server</i> DNS	18



3.2.5	Perancangan Memcached.....	19
3.2.6	Metode Pembuatan Program Python	20
3.2.7	Perancangan ELK Stack	26
3.2.8	Metode Pembuatan <i>Filter</i>	31
3.2.9	Visualisasi	33
3.2.10	Metode Pengujian	42
BAB IV	45
4.1	Hasil Analisis dan Pengolahan Data Log pada Logstash	45
4.1.1	Hasil Data Log “Normal”	45
4.1.2	Hasil Data Log “Threat”	46
4.2	Hasil Penguraian dan <i>Lookup</i> Data Log pada Elasticsearch	51
4.3	Hasil Visualisasi pada <i>Dashboard</i> Kibana	52
4.3.1	<i>Sum of DNS Request</i>	53
4.3.2	<i>Count Request</i>	53
4.3.3	<i>Threat Recorded</i>	54
4.3.4	<i>Query Type</i>	55
4.3.5	<i>Destinationn of Client Request</i>	55
4.3.6	<i>Client IP</i>	56
4.3.7	<i>Top 5 IP/Domain Requested</i>	56
4.3.8	<i>Threat Information</i>	57
4.3.9	<i>Correlation event -1 dan Correlation event -2.</i>	57
BAB V	59
5.1	Kesimpulan.....	59
5.2	Saran	59
DAFTAR PUSTAKA	60