



## DAFTAR ISI

HALAMAN JUDUL .....	i
LEMBAR PENGESAHAN .....	iii
PERNYATAAN BEBAS PLAGIASI .....	iv
KATA PENGANTAR .....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xi
INTISARI .....	xiii
<i>ABSTRACT</i> .....	xiv
BAB I PENDAHULUAN.....	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.....	2
1.6. Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA .....	4
2.1. Penelitian Acuan .....	4
2.2. Landasan Teori.....	10
2.2.1. <i>Cyber Threat</i> .....	10
2.2.2. Penilaian Ancaman .....	10
2.2.3. Penilaian Kuantitatif .....	10
2.2.4. <i>Indicator of Compromise</i> .....	11
2.2.5. Taksonomi Insiden.....	11
2.2.6. <i>Cyber Threat Intelligence</i> .....	11
2.2.7. Malware Information Sharing Platform.....	12
2.3. Hipotesis.....	13
BAB III METODE PENELITIAN .....	14
3.1. Alat dan Bahan.....	14
3.1.1. Perangkat Keras .....	14
3.1.2. Perangkat Lunak .....	14
3.2. Prosedur Penelitian.....	15
3.2.1. Arsitektur Sistem Keseluruhan .....	15
3.2.2. Arsitektur Sistem pada Fokus Penelitian .....	16



3.2.3	Alur Penelitian .....	17
3.2.3.1	Penentuan Taksonomi .....	17
3.2.3.2	Penentuan Metode Penilaian .....	21
3.2.3.4	Perhitungan <i>Predicate's Weight</i> .....	79
3.2.3.5	Perhitungan <i>Namespace Weight</i> .....	83
3.2.4	Normalisasi Hasil Perhitungan .....	86
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....		90
4.1.	CERT-XLM, CIRCL, ECSIRT, Europol-Incident, RSIT.....	90
4.2.	Malware_Classification.....	98
4.3.	Ms-CARO-Malware.....	100
4.4.	Analisis Hasil Perhitungan .....	101
BAB V PENUTUP .....		104
5.1.	Kesimpulan.....	104
5.2.	Saran.....	104
DAFTAR PUSTAKA .....		105
LAMPIRAN.....		114