

## DAFTAR ISI

HALAMAN JUDUL .....	i
<b>LEMBAR PENGESAHAN .....</b>	<b>iii</b>
PERNYATAAN BEBAS PLAGIASI .....	iv
KATA PENGANTAR .....	v
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xiv
INTISARI .....	xv
ABSTRACT.....	xvi
<b>1 BAB I.....</b>	<b>1</b>
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
<b>BAB II.....</b>	<b>1</b>
1.1 <i>Honeypot</i> .....	6
1.2 <i>Dionaea Honeypot</i> .....	6
1.3 <i>Cyber Threat Intelligence</i> .....	6
1.4 <i>Malware Information Sharing Platform (MISP)</i> .....	6
1.5 Taksonomi .....	6
1.6 <i>Selenium</i> .....	7
1.7 <i>Pandas</i> .....	7
1.8 Hipotesis .....	7

<b>BAB III</b>	8
3.1 Bahan.....	8
3.2 Peralatan .....	8
3.3 Arsitektur Sistem Keseluruhan.....	9
3.3.1 Komponen SIEM ( <i>Security Information and Event Management</i> ) .....	10
3.3.2 Komponen SOAR ( <i>Security, Orchestration, Automation, and Response</i> ) .....	12
3.4 Metode Automasi pada MISP .....	13
3.5 Arsitektur Sistem pada Fokus Penelitian .....	14
3.6 Metode Penilaian pada IoC .....	16
3.6.1. <i>Base Score</i> .....	18
3.6.2. <i>Emersion</i> .....	18
3.6.3. <i>MISP Score</i> .....	19
3.6.4. <i>Tags</i> .....	19
3.7 Skenario Contoh Penilaian pada IoC .....	20
3.7.1. Skenario.....	20
3.7.2. Menentukan nilai <i>Brute-force Attack Rate</i> .....	20
3.7.3. Menghitung nilai <i>tags</i> .....	22
3.7.4. Menghitung nilai <i>misp_score</i> .....	23
3.7.5. Menghitung <i>emersion</i> kemunculan pertama ( $n = 0$ ) .....	24
3.7.6. Menghitung <i>base_score</i> kemunculan pertama .....	24
3.7.7. Menghitung <i>emersion</i> kemunculan kedua ( $n = 1$ ).....	24
3.7.8. Menghitung <i>base_score</i> kemunculan kedua.....	24
<b>BAB IV</b> .....	25
4.1. Implementasi MISP.....	25
4.2. Implementasi <i>Honeypot</i> Dionaea .....	30
4.3. Konfigurasi <i>Logging</i> pada Dionaea .....	30
4.4. Konfigurasi dan <i>Testing</i> pada <i>Service</i> Dionaea.....	32

4.4.1.	SMB.....	32
4.4.2.	FTP.....	36
4.4.3.	HTTP.....	37
4.4.4.	MYSQL.....	39
4.4.5.	MQTT .....	41
4.4.6.	MongoDB .....	43
4.4.7.	SIP.....	45
4.4.8.	MSSQL .....	46
4.4.9.	UPNP .....	48
4.4.10.	PPTP.....	49
4.5.	Implementasi <i>Harvester</i> .....	50
4.6.	Implementasi <i>Collector</i> .....	52
4.7.	Implementasi <i>Profiler</i> .....	55
4.8.	Implementasi MongoDB .....	73
4.9.	Implementasi Elastic Stack .....	74
4.10.	Hasil Sistem.....	77
4.10.1.	Visualisasi Data.....	77
4.10.2.	Hasil Pengujian .....	81
BAB V	.....	83
5.1	Kesimpulan.....	83
5.2	Saran.....	83
DAFTAR PUSTAKA	.....	84