

DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR	i
PENGESAHAN PENGUJI SIDANG TUGAS AKHIR.....	ii
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR	iii
<i>ABSTRACT</i>	iv
ABSTRAK	v
HALAMAN MOTTO DAN PERSEMBAHAN.....	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
DAFTAR LAMPIRAN	xiv
BAB 1 PENDAHULUAN	I-1
1.1. Latar Belakang.....	I-1
1.2. Rumusan Masalah	I-4
1.3. Tujuan Penelitian.....	I-4
1.4. Manfaat Penelitian.....	I-4
1.5. Batasan Masalah.....	I-5
BAB II LANDASAN TEORI	I-1
2.1 Security Information and Event Management (SIEM)	II-1
2.2 Cyber Threat Intelligence	II-1
2.3 <i>Wazuh</i>	II-2

2.4	Malware Information Sharing Platform (<i>MISP</i>).....	II-7
2.5	DFIR-IRIS	II-7
2.6	Penelitian Terkait.....	II-8
2.7	Keterbaruan Penelitian	II-14
BAB III METODOLOGI PENELITIAN.....		III-1
3.1	Tahapan Penelitian	III-1
3.2	Analisis Kebutuhan Sistem.....	III-2
3.3	Perancangan Sistem.....	III-4
3.4	Implementasi Sistem	III-5
3.5	Pengujian Sistem	III-6
3.6	Analisis Hasil Pengujian.....	III-7
BAB IV HASIL DAN PEMBAHASAN		IV-1
4.1.	Implementasi Sistem	IV-1
4.1.1.	Konfigurasi dan Instalasi <i>Wazuh</i>	IV-1
4.1.2.	Instalasi dan Konfigurasi <i>MISP</i>	IV-5
4.1.3.	Instalasi dan Konfigurasi DFIR -IRIS.....	IV-13
4.1.4.	Deploy <i>Wazuh</i> Agent Pada Host	IV-17
4.2.	Pengujian Sistem	IV-19
4.2.1.	Pengujian <i>WAZUH</i>	IV-19
4.2.2.	Pengujian <i>Wazuh</i> dan <i>MISP</i>	IV-21
4.2.3.	Pengujian <i>Wazuh</i> , DFIR-Iris dan <i>MISP</i>	IV-23
4.3.	Analisis Hasil Pengujian.....	IV-24

BAB V KESIMPULAN DAN SARAN.....	V-1
5.1. Kesimpulan.....	V-1
5.2. Saran.....	V-2
DAFTAR PUSTAKA	
LAMPIRAN LAMPIRAN	

DAFTAR GAMBAR

Gambar 2. 1 Logo WAZUH.....	II-3
Gambar 2. 2 Arsitektur WAZUH.....	II-3
Gambar 3. 1 Diagram Alur Penelitian.....	III-1
Gambar 3. 2 Topologi Sistem	III-4
Gambar 3. 3 Gambaran Cara Kerja Sistem.....	III-5
Gambar 4. 1 Konfigurasi WAZUH.....	IV-2
Gambar 4. 2 Tampilan Login Page Wazuh.....	IV-4
Gambar 4. 3 Homepage Wazuh	IV-4
Gambar 4. 4 Konfigurasi Virustotal.....	IV-5
Gambar 4. 5 Instalasi MISP	IV-6
Gambar 4. 6 Tampilan login Page MISP	IV-7
Gambar 4. 7 Penambahan Feeds pada MISP	IV-8
Gambar 4. 8 Feeds MISP	IV-9
Gambar 4. 9 Auth key MISP.....	IV-9
Gambar 4. 10 Konfigurasi custom-MISP.....	IV-10
Gambar 4. 11 Integrasi Pada WAZUH	IV-12
Gambar 4. 12 Integrasi Berhasil.....	IV-13
Gambar 4. 13 Instalasi DFIR-Iris.....	IV-14
Gambar 4. 14 Script Integrasi DFIR-IRIS	IV-15
Gambar 4. 15 Konfigurasi WAZUH untuk integrasi DFIR-iris	IV-16
Gambar 4. 16 Alert WAZUH Pada DFIR-IRIS	IV-17
Gambar 4. 17 Deploy WAZUH Agent	IV-18
Gambar 4. 18 Grafik Pengujian Wazuh	IV-21
Gambar 4. 19 Grafik Pengujian Wazuh dan MISP	IV-22
Gambar 4. 20 Alert Pada DFIR-IRIS.....	IV-24
Gambar 4. 21 Grafik Hasil Evaluasi Matriks.....	IV-26

DAFTAR TABEL

Tabel 2. 1 Perbandingan SIEM	II-5
Tabel 2. 2 Penelitian Terkait	II-8
Tabel 2. 3 Matriks Penelitian	II-14
Tabel 3. 1 Kebutuhan Hardware	III-2
Tabel 3. 2 Kebutuhan Software.....	III-3
Tabel 4. 1 Hasil Pengujian Wazuh.....	IV-20
Tabel 4. 2 Hasil Pengujian Wazuh+MISP	IV-21
Tabel 4. 3 Hasil Evaluasi Pengujian	IV-24

DAFTAR LAMPIRAN

Lampiran 1.	Daftar Istilah.....	L1-1
Lampiran 2.	Surat Keterangan Tugas Akhir	L2-1
Lampiran 3.	Lembar Mengikuti Sidang Seminar Hasil	L3-1
Lampiran 4.	Lembar Konsultasi Tugas Akhir	L4-1
Lampiran 5.	Revisi Laporan Sidang Usulan Penelitian	L5-1
Lampiran 6.	Revisi Laporan Seminar Hasil.....	L6-1
Lampiran 7.	Lembar Daftar Hadir Seminar Hasil.....	L7-1
Lampiran 8.	Lembar Rekap Perbaikan Seminar Hasil.....	L8-1
Lampiran 9.	Lembar Revisi Laporan Tugas Akhir	L9-1
Lampiran 10.	Lembar Rekap Perbaikan Tugas Akhir	L10-1