

DAFTAR GAMBAR

Gambar 2. 1 Logo CTI Group	5
Gambar 2. 2 Logo Defenxor	7
Gambar 2. 3 Struktur jabatan Defenxor	7
Gambar 2. 4 Service DIMS	8
Gambar 2. 5 Service DISC	9
Gambar 2. 6 Service DISI	10
Gambar 2. 7 Flowchart	13
Gambar 3. 1 TTP (Tactics, Technique, procedure)	16
Gambar 3. 2 Evidence 1	17
Gambar 3. 3 Evidence 2	18
Gambar 3. 4 Evidence 3	18
Gambar 3. 5 Evidence 4	19
Gambar 3. 6 Evidence 5	20
Gambar 3. 7 Evidence 6	21
Gambar 3. 8 Evidence 7	21
Gambar 3. 9 Evidence 8	22
Gambar 3. 10 Evidence 9	23
Gambar 3. 11 Evidence 10	24
Gambar 3. 12 Evidence 11	26
Gambar 3. 13 Evidence 12	26
Gambar 3. 14 Evidence 13	27
Gambar 3. 15 Evidence 14	27
Gambar 3. 16 Evidence 15	27
Gambar 3. 17 Evidence 16	28
Gambar 3. 18 Evidence 17	28
Gambar 3. 19 Evidence 18	29
Gambar 3. 20 Evidence 19	29
Gambar 3. 21 Evidence 20	30
Gambar 3. 22 Evidence 21	30
Gambar 3. 23 Evidence 22	31
Gambar 3. 24 Evidence 23	31
Gambar 3. 25 Evidence 24	32
Gambar 3. 26 Evidence 25	32
Gambar 3. 27 Evidence 26	33
Gambar 3. 28 Evidence 27	33
Gambar 3. 29 Flow attack	45
Gambar 3. 30 Tampilan Dsiem	49
Gambar 3. 31 Tampilan Elastic Search	50

Gambar 3. 32 Tampilan OpenSearch	51
Gambar 3. 33 Tampilan Arkime	52
Gambar 3. 34 Website AbuseIPDB	53
Gambar 3. 35 Website VirusTotal.....	53
Gambar 3. 36 Website Cisco Talos.....	54
Gambar 3. 37 Website Spamhaus	54
Gambar 3. 38 Website Kaspersky OpenTIP	55
Gambar 4. 1 Perancangan sistem	57
Gambar 4. 2 Aktifkan WSL.....	59
Gambar 4. 3 Script WSL	59
Gambar 4. 4 Konfigurasi Elasticsearch.....	60
Gambar 4. 5 Konfigurasi Wazuh Manager.....	62
Gambar 4. 6 Integrasi MITRE ATT&CK.....	63
Gambar 4. 7 Konfigurasi NGINX	64
Gambar 4. 8 Konfigurasi Filebeat	65
Gambar 4. 9 Konfigurasi filebeat wazuh json.....	66
Gambar 4. 10 Percobaan VM Windows	67
Gambar 4. 11 Hasil pada Elasticsearch	68
Gambar 4. 12 Hasil pada Elasticsearch 2.....	68
Gambar 4. 13 Hasil MITRE ATT&CK.....	69