

## DAFTAR ISI

---

KATA PENGANTAR .....	i
ABSTRAK .....	ii
ABSTRACT .....	iii
DAFTAR ISI .....	iv
DAFTAR GAMBAR .....	vii
DAFTAR TABEL .....	ix
BAB 1 PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah dan Solusi .....	2
1.3 Tujuan .....	2
1.4 Batasan Masalah .....	3
1.5 Penjadwalan Kerja Dan Timeline Penelitian .....	3
BAB 2 TINJAUAN PUSTAKA .....	5
2.1 Tinjauan Pustaka .....	5
2.2 Perusahaan CTI Group .....	6
2.3 Gambaran umum Instansi .....	7
2.4 Unit Kerja .....	11
BAB 3 ANALISIS DAN PERANCANGAN .....	14
3.1 Analisis Deskripsi dan Alur Pekerjaan .....	14
3.2 Analisis Aktivitas Mining Monero Secara Legal .....	15
3.3 Gambaran Sistem Saat Ini .....	16
3.3.1 Pengumpulan Data dan Parsing Log .....	17
3.3.2 Normalisasi Log .....	17

3.3.3 Pengiriman ke DSIEM dan Elasticsearch .....	17
3.3.4 Korelasi dan Pembentukan Alarm .....	17
3.3.5 Pengiriman Alarm ke Elasticsearch .....	17
3.4 Kebutuhan Perangkat Kerja .....	18
3.4.1 DSIEM (Defenxor Security Information and Event Management .....	18
3.4.2 Kibana OpenSearch .....	19
3.4.3 Wazuh Manager .....	20
3.4.4 Arkime Packet Capture .....	21
3.4.5 Icinga Dashboard .....	22
3.4.6 Thruk Dashboard .....	23
3.4.7 Intelijen Ancaman (Threat Intelligence) .....	24
<b>BAB 4 IMPLEMENTASI DAN PENGUJIAN .....</b>	<b>29</b>
4.1 Implementasi .....	29
4.1.1 Initial Access (Akses Awal) .....	30
4.1.2 Execution (Eksekusi) .....	31
4.1.3 Persistence (Ketahanan) .....	31
4.1.4 Defense Evasion (Penghindaran Deteksi) .....	31
4.1.5 Credential Access (Akses Kredensial) .....	31
4.1.6 Discovery (Penemuan) .....	31
4.1.7 Lateral Movement (Pergerakan Lateral) .....	32
4.1.8 Command and Control (C2) .....	32
4.1.9 Exfiltration (Eksfiltrasi Data) .....	32
4.1.10 Impact (Dampak) .....	32
4.2 Analisis Aktivitas Dari Monero Cryptocurrency .....	32
4.2.1 Konfigurasi Pada Sistem .....	33
4.2.2 Pengecekan Pada Log Traffic .....	34

4.2.3 Pengecekan Pada Perangkat .....	36
4.2.4 Pengecekan Threat Intelligence .....	37
4.2.5 Remediasi dan Pengecekan Pada Host .....	39
4.2.6 Konfigurasi Rules Pada Firewall .....	40
4.3 Hasil Akhir .....	41
<b>BAB 5 KESIMPULAN .....</b>	<b>45</b>
5.1 Kesimpulan .....	45
5.2 Saran .....	45
<b>DAFTAR PUSTAKA .....</b>	<b>47</b>