DAFTAR ISI

LEMBAR PERSEMBAHAN i
LEMBAR PENGESAHAN i
LEMBAR PENGESAHAN PEMBIMBING LAPANGAN MAGANG ii
KATA PENGANTAR iii
PERNYATAAN iv
ABSTRAK v
ABSTRACT vi
DAFTAR ISI vii
DAFTAR GAMBAR x
DAFTAR TABEL xii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah dan Solusi 2
1.3 Tujuan 3
1.4 Penjadwalan Kerja 4
BAB II PROFIL ORGANISASI 5
2.1 Deskripsi Organisasi 5
2.2 Struktur Organisasi dan Tata Kelola 6
2.3 Deskripsi Pekerjaan 10
BAB III ANALISIS PEKERJAAN 15
3.1 Analisis Sistem 15
3.2.1. Analisis Ancaman Berdasarkan Kerangka *MITRE ATT&CK* 16
3.2.1.1 Aktivitas mencurigakan *successful login activity (MITRE ATT&CK ID: T1078)* 17
3.2.1.2 *Logon used explicit credentials with special privileges assigned to the new session (MITRE ATT&CK ID: T1548.002).* 18
3.2.1.3 *Service Start (MITRE ATT&CK ID: T1543.003)* 19
3.2.1.4 *Group Membership change* (*MITRE ATT&CK ID: T1069*) 21

3.2.1.5 *Account Preparation for Running Monkey Island (MITRE ATT&CK ID: T1098)* 21
3.2.1.6 *Authentication and Credential Validation Event* (*MITRE ATT&CK ID: T1548*) 22
3.2.1.7 *File Creation* (*MITRE ATT&CK ID: T1027*) 23
3.2.1.8 *Cleaning Traces After Running Monkey Island* (*MITRE ATT&CK ID: T1098)* 24
3.2.1.9 *System Services: Service Execution* (*MITRE ATT&CK* ID: *T1569.002*) 26
3.2.1.10 *Brute Force: SSHD* (*MITRE ATT&CK: T1021*) 27
3.2.1.11 *Web Attack and Exfiltration (MITRE ATT&CK: T1041)* 28
3.2.1.12 *Logon Failure* (*MITRE ATT&CK: T1110*) 29
3.2.1.13 *User Execution* (*MITRE ATT&CK: T1098 dan MITRE ATT&CK ID: T1548*) 30
3.2.1.14 *Network Scanning (MITRE ATT&CK: T1046)* 31
3.2.1.15 *Lateral Movement (MITRE ATT&CK: TA0008)* 32
3.2.1.16 Analisis pada *Threat Intelligence (MITRE ATT&CK: T1027)* 33
3.2.2. Strategi Mitigasi Keamanan dengan *CIS Control* 34
3.2.2.1 *CIS Control 1 Inventory and Control of Enterprise Assets* 34
3.2.2.2 *CIS Control 2 Inventory and Control of Software Assets* 35
3.2.2.3 *CIS Control* 3 *Data Protection* 35
3.2.2.4 *CIS Control* 4 *Secure Configuration of Enterprise Assets and Software* 36
3.2.2.5 *CIS Control* 5 *Account Management* 37
3.2.2.6 *CIS Control* 6 *Access Control Management* 38
3.2.2.7 *CIS Control* 7 *Continuous Vulnerability Management* 38
3.2.2.8 *CIS Control* 8 *Audit Log Management* 39
3.2.2.9 *CIS Control* 9 *Email and Web Browser Protections* 40
3.2.2.10 *CIS Control* 16 *Application Software Security* 40
3.2.2.11 *CIS Control* 17 *Incident Response Management* 41
3.2 Dampak Serangan Infection Monkey, Rekomendasi, dan Strategi Mitigasi ... 42
3.3 Kebutuhan Perangkat Kerja 49
BAB IV HASIL DAN PEMBAHASAN 56
4.1 Hasil Akhir 56

4.2 Pengujian Luaran 66
BAB V KESIMPULAN DAN SARAN 70
5.1 Kesimpulan 70
5.2 Saran 70
DAFTAR PUSTAKA 72
LAMPIRAN 74