

DAFTAR GAMBAR

Gambar 1. 1 Gedung Graha Mandiri.....	3
Gambar 2. 1 Logo Perusahaan NOOSC.....	5
Gambar 2. 2 Struktur Organisasi Perusahaan NOOSC.....	6
Gambar 2. 3 Kegiatan Umum Perusahaan NOOSC	8
Gambar 3. 1 Arsitektur SOC	12
Gambar 3. 2 Health Check Qradar	17
Gambar 3. 3 Pengisian Hasil Health Check Qradar	17
Gambar 3. 4 Health Check Alienvault	18
Gambar 3. 5 Pengisian Hasil Health Check Alienvault.....	18
Gambar 3. 6 Dashboard Penarikan Data dari Qradar Panorama	19
Gambar 3. 7 Dashboard Penarikan Data dari Qradar Wincollect	19
Gambar 3. 8 Template Laporan Operasional Qradar	20
Gambar 3. 9 Pengiriman Laporan melalui Telegram.....	20
Gambar 3. 10 Dashboard Penarikan Data Splunk untuk Sophos.....	21
Gambar 3. 11 Dashboard Penarikan Data Splunk untuk Trend Micro	21
Gambar 3. 12 Template Laporan Splunk	22
Gambar 3. 13 Pengiriman Laporan Melalui WhatsApp	23
Gambar 3. 14 Laporan Status Tiket.....	23
Gambar 3. 15 Praktikan Memeriksa Suhu dan Kelembapan.....	24
Gambar 3. 16 Pengisian Hasil Pemeriksaan Suhu dan Kelembapan.....	24
Gambar 3. 17 Report Sophos	26
Gambar 3. 18 Report Trend Micro	26
Gambar 3. 19 Tampilan Alert dari Alienvault.....	27
Gambar 3. 20 Tampilan Detail Event dari Alert	28
Gambar 3. 21 Template Laporan Alienvault.....	28
Gambar 3. 22 Praktikan saat menjadi SOC Analyst.....	29
Gambar 3. 23 Tampilan dari Pesan First Detection.....	31
Gambar 3. 24 Tampilan dari Pesan Analysis	31
Gambar 3. 25 Tampilan OWLH NIDS nodes.....	32
Gambar 3. 26 Pengisian Hasil Health Check NIDS.....	32
Gambar 3. 27 Ticketing Summary	33
Gambar 3. 28 Aktivitas Pada SIEM.....	33
Gambar 3. 29 Tampilan Dashboard Active Directory Monitoring.....	34
Gambar 3. 30 Tampilan Query Search di Splunk	35
Gambar 3. 31 Save Panel to Existing Dashboard	38
Gambar 3. 32 Tampilan Multiple Failed Login Acces During Off-hours	38
Gambar 3. 33 Tampilan Total Succes Authentication dan Failed	39
Gambar 3. 34 Tampilan Event Detail Success and Failed	40
Gambar 3. 35 Visualisasi Tiket Sophos Mingguan	42
Gambar 3. 36 Data yang Praktikan Olah Untuk Visualisasi.....	43
Gambar 3. 37 Visualisasi Data Sophos.....	44
Gambar 3. 38 Panduan Teknis Oleh Praktikan	45

Gambar 3. 39 Praktikan Saat Melakukan Dismantle Server.....	46
Gambar 3. 40 Tampilan SIEM Wazuh.....	47
Gambar 3. 41 OS Kali Linux yang digunakan	47
Gambar 3. 42 Spesifikasi Hardware dari VM	48
Gambar 3. 43 Wazuh Agent yang sudah dikonfigurasi	49
Gambar 3. 44 Simulasi Penyerangan ke Wazuh.....	49
Gambar 3. 45 Alert yang Muncul Dari Penyerangan	50
Gambar 3. 46 Hasil Server yang Dibuat.....	50
Gambar 3. 47 Pfsense di VM.....	51
Gambar 3. 48 Dashboard pfSense	51
Gambar 3. 49 Praktikan saat Meeting Dengan Pembimbing Kerja.....	53
Gambar 3. 50 User Memberikan List Asset.....	53
Gambar 3. 51 Materi Ethical Hacking.....	54
Gambar 3. 52 Praktikan Melakukan VA	55
Gambar 3. 53 Laporan Proposal VA	56
Gambar 3. 54 Praktikan Presentasi Dengan User dan Pembimbing.....	57
Gambar 3. 55 Praktikan melakukan Revisi Proposal	57
Gambar 3. 56 Praktikan Presentasi terkait Hasil Laporan	58

