

## DAFTAR GAMBAR

---

|   |    |
|---|----|
| Gambar 2. 1 Logo CTI Group .....  | 6  |
| Gambar 2. 2 Logo Defenxor .....   | 7  |
| Gambar 2. 3 Struktur Jabatan Defenxor .....   | 8  |
| Gambar 2. 4 Logo Defenxor Intelligence Managed Security .....                           | 9  |
| Gambar 2. 5 Logo Defenxor Intelligence Security Consulting .....                        | 10 |
| Gambar 2. 6 Logo Defenxor Intelligence Security Integrator .....                        | 11 |
| Gambar 3. 1 Flowchart alur pekerjaan .....  | 14 |
| Gambar 3. 2 Diagram Alur Pengolahan Log Sistem Saat Ini .....                           | 16 |
| Gambar 3. 3 DSIEM (Defenxor Security Information and Event Management) .....            | 18 |
| Gambar 3. 4 Kibana OpenSearch .....   | 19 |
| Gambar 3. 5 Wazuh manager .....   | 20 |
| Gambar 3. 6 Arkime Packet Capture .....   | 21 |
| Gambar 3. 7 Incinga Dashboard .....   | 22 |
| Gambar 3. 8 Thruk Dashboard .....   | 23 |
| Gambar 3. 9 Virus Total .....   | 25 |
| Gambar 3. 10 AbuseIPDB .....  | 25 |
| Gambar 3. 11 Kaspersky Opentip .....  | 25 |
| Gambar 3. 12 EmailHunter .....  | 26 |
| Gambar 3. 13 ThreatBook CTI .....   | 26 |
| Gambar 3. 14 MXToolBox .....  | 27 |
| Gambar 3. 15 MacVendor .....  | 27 |
| Gambar 3. 16 OTX AlienVault .....   | 27 |
| Gambar 3. 17 IPQualityScore .....   | 28 |
| Gambar 4. 1 Command Pengecekan Konfigurasi Pada Sistem .....                            | 34 |
| Gambar 4. 2 Adanya Aktivitas Massive Berasal dari Luar Menuju Port 22 .....             | 34 |
| Gambar 4. 3 Adanya Aktivitas dari Internal yang Melakukan Query ke Arah Luar .....      | 35 |
| Gambar 4. 4 Grafik Pengecekan Pada Sistem Firewall .....                                | 36 |
| Gambar 4. 5 Adanya Aktivitas Malicious menggunakan port DNS yang bersifat massive ..... | 36 |
| Gambar 4. 6 Pengecekan Perangkat yang Terdampak .....                                   | 37 |

|  |    |
|--|----|
| Gambar 4. 7 Pengecekan IP pada Threat Intelligence AbuseIP .....             | 37 |
| Gambar 4. 8 Pengecekan ThreatBook Intelligence .....                         | 38 |
| Gambar 4. 9 Pengecekan Pada Task Manager Milik Host Terdampak .....          | 39 |
| Gambar 4. 10 Melakukan Blocking Pada Firewall Untuk Aktivitas Outbound ..... | 40 |
| Gambar 4. 11 Grafik System CPU Usage Pada Perangkat Terdampak .....          | 40 |