BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Pada penelitian kali ini didapat 3 kesimpulan yang menjadikan pondasi keberhasilan penetelitian ini diantaranya :

1. LogRhythm dengan CrowdStrike Falcon lebih unggul dalam deteksi berbasis machine learning dan analisis, yang memungkinkan identifikasi ancaman baru meskipun belum terdaftar dalam database malware. Sementara itu, Wazuh dengan integrasi VirusTotal lebih berfokus pada deteksi berbasis hash dan reputasi file, memberikan transparansi dengan hasil dari berbagai mesin antivirus.
2. Wazuh lebih fleksibel dan transparan karena memungkinkan pengguna untuk mengakses hasil deteksi tanpa biaya tambahan, sedangkan LogRhythm dengan CrowdStrike Falcon sering kali memerlukan biaya tambahan untuk mendapatkan laporan analisis yang lebih rinci. Ini menjadikan Wazuh lebih ideal untuk organisasi yang mengutamakan keterbukaan dalam analisis ancaman tanpa investasi tambahan.
3. Hasil penelitian ini adalah dengan membandingkan kedua SIEM yang digunakan pada perusahaan, didapatkan hasil dengan menunjukan *wazuh* dapat menjadi pesaing dengan *logrhythm*. dengan membandingkan beberapa fitur yang ada pada kedua SIEM tersebut, wazuh dapat lebih unggul dengan logrhythm dikarenakan *wazuh* yang bersifat open source dapat dimodifikasi sedemikian rupa mengikuti keinginan pengguna.

5.2 Saran

Saran dari penulis untuk peneliti selanjutnya, dicoba untuk *malware* versi terbaru, dikarenakan saat ini *malware* yang digunakan adalah malware terbaru selama 4 bulan penelitian. Dimulai dari bulan November – Februari.