ABSTRAK

Lembaga pemerintahan di Indonesia semakin rentan terhadap ancaman siber yang canggih, seperti *phishing*, *ransomware*, serangan DDoS, dan *advanced persistent threats* (APT). Ancaman ini memanfaatkan berbagai keterbatasan institusional, termasuk tata kelola yang terfragmentasi, kapasitas teknis yang rendah, dan infrastruktur lama. Model *Security Operations Center* (SOC) yang ada saat ini umumnya bersifat kompleks, bergantung pada vendor, dan tidak sesuai dengan kondisi operasional sektor publik di Indonesia. Penelitian ini mengusulkan model SOC modular berbasis tier yang disesuaikan dengan keterbatasan dan kebutuhan institusional pemerintah. Dengan menggunakan metodologi *Design Science Research* (DSR), studi ini melalui enam tahap sistematis: eksplisitasi masalah, definisi kebutuhan melalui tinjauan literatur sistematis, desain awal model, validasi dan penyempurnaan melalui masukan ahli, demonstrasi pada pemerintah daerah, serta evaluasi terstruktur. Hasil penelitian menghasilkan SOC Model v1.0 dengan kapabilitas bertingkat (Tier 1–3) dan tujuh komponen inti yaitu Orang, Proses, Teknologi, Tata Kelola, Kolaborasi, Metrik, dan Inovasi. Validasi oleh para ahli dan praktisi pemerintahan menunjukkan bahwa model ini relevan, layak diterapkan, dan dapat diskalakan. Kontribusi teoretis dari penelitian ini adalah pengayaan literatur tentang desain SOC sektor publik melalui integrasi kerangka internasional (NIST CSF, MITRE ATT&CK) dalam konteks lokal. Secara praktis, model ini memberikan kerangka kerja siap pakai yang sesuai dengan kapasitas organisasi dan dapat menjadi alternatif terhadap model SOC yang bersifat komersial dan seragam. .

Kata kunci: Keamanan Siber, Pemerintahan, Security Operations Center, Modular SOC, Model SOC Berbasis Tier