# ABSTRAK

Keamanan data merupakan aspek penting dari kemajuan teknologi informasi di era digital ini. Meskipun upaya keamanan data terus meningkat, kebocoran data tetap menjadi ancaman signifikan. Penggunaan OSINT menjadi alat yang sangat berguna untuk membantu dalam mitigasi *phishing attack* menggunakan metode *auditing and policy based* dengan melakukan aktivitas *Social Engineering* dan eksperimen menggunakan teknik *spear phishing* pada konten *email*. Hal ini dapat digunakan untuk mengidentifikasi celah keamanan yang mungkin perlu diperbaiki. Dengan menerapkan teknik tersebut, dapat memperoleh gambaran yang lebih jelas mengenai potensi titik lemah pada sistem yang digunakan. Penelitian ini melakukan implementasi eksperimen menggunakan OSINT *tools*, aktivitas *social engineering*, dan konten *email*. Eksperimen OSINT dan *phishing attack* disajikan dalam bentuk *Data Flow Diagram* untuk menunjukkan alur dari serangan yang dilakukan. Pada eksperimen konten *email* dirumuskan menggunakan *Activity Diagram* yang digunakan untuk memvisualisasikan langkah-langkah mitigasi menggunakan metode *auditing and policy based*. Metode ini mencakup penerapan *continuous auditing* dan kebijakan seperti UU PDP dan rancangan SOP yang tepat dalam menjaga keamanan data dalam menghadapi serangan *phishing*. Dengan mengintegrasikan *auditing and policy* memungkinkan penerapan strategi mitigasi yang lebih terstruktur dan berorientasi pada hasil yang efektif untuk melindungi data dari potensi kebocoran dan memperkuat sistem keamanan secara menyeluruh.

Kata kunci—**OSINT, *Phishing, Social Engineering, Auditing and Policy Based***