Pengembangan Kemampuan Kontra Intelijen Siber di Pusat Operasi Keamanan Siber Nasional untuk mewujudkan Ketahanan Nasional dalam mengatasi Ancaman Siber di Indonesia = Development of the capabilities of the Cyber Counter Intelligence at the National Cyber Security Operations Center to realize National Resilience in overcoming the Cyber Threat in Indonesia.

Abdul Hakim Nur Maulana, author

Abstrak

ABSTRAK
Pada tahun 2018, diketahui terjadi sebanyak 232,447,974 serangan siber ke jaringan Indonesia. Sektor yang menjadi perhatian adalah instansi pemerintah, karena menjadi target utama serangan siber. Domain .go.id (website pemerintah) menempati peringkat pertama dengan 30,75% lebih sering terkena defacement. Untuk mengatasi masalah ancaman siber, Pemerintah Indonesia membentuk BSSN, yang mempunyai unit kerja Pusopskamsinas, yang kemudian telah membentuk Secuity Operation Center (SOC). Namun SOC yang sudah dibentuk belum sesuai kebutuhan, yang ada saat ini belum cukup karena lingkup, maturitas dan kapabilitas SOC masih terbatas, sedangkan ancaman siber setiap detik selalu berkembang, dibutuhkan kemampuan kontra intelijen siber sebagai langkah dan strategi intelijen untuk memprediksi dan menanggulangi kemungkinan ancaman siber, serta membangun pola koordinasi dengan SOC lainnya untuk mewujudkan Collaborative Cyberdefense. Maka dibentuklah National Secuity Operation Center (NSOC), yaitu pengembangan dari SOC yang memerlukan upaya rencana pembangunan keamanan siber yang terukur untuk menjamin keberhasilaln tugas dan fungsinya. Oleh karena itu, pada penelitian ini akan dilakukan pengembangan kemampuan kontra intelijen siber di Pusopskamsinas menggunakan langkah kerangka kerja keamanan siber berdasarkan NIST CSF, yang dipadukan dengan Penilaian maturitas dan kapabilitas pada SOC di Pusopskamsinas menggunakan SOC-CMM, serta rekomendasi rencana aksi menggunakan konsep kontra intelijen siber.
<hr>
ABSTRACT
In 2018, there were 232,447,974 cyber attacks on the Indonesian network. The sector of concern is government agencies, because they are the main target of cyber attacks. Domain. Go.id (government website) ranks first with 30.75% more often affected by defacement. To overcome the problem of cyber threats, the Government of Indonesia formed BSSN, which has a work unit of Pusopskamsinas, which then has formed the Secuity Operation Center (SOC). However, the SOC that has been formed is not yet in accordance with the needs, which is currently not enough because the scope, maturity and capability of the SOC is still limited, while cyber threats are always developing every second, cyber counterintelligence capabilities are needed as a step and intelligence strategy to predict and cope with possible cyber threats , and build coordination patterns with other SOCs to realize Collaborative Cyberdefense. Then a National Secuity Operation Center (NSOC) was formed, which is the development of an SOC that requires measurable cyber security development plans to ensure the success of its duties and functions. Therefore, this research will develop the capacity of cyber counterintelligence in Pusopskamsinas using the steps of the

cyber security framework based on NIST CSF, which is integrated with the assessment of maturity and capability in SOC in Pusopskamsinas using SOCCMM, and recommendations for action plans using cyber counter intelligence concepts cyber.