# Perancangan Kerangka Kerja "National Security Operation Center-Vulnerability Management" (NSOC-VM) untuk Melindungi Infrastruktur Informasi Vital = Design of the "National Security Operation Center-Vulnerability Management" (NSOC-VM) Framework to Protect Critical Information Infrastructure

Muhammad Azza Ulin Nuha, author



---

Abstrak

Keamanan siber merupakan aspek penting dalam penyelenggaraan Infrastruktur Informasi Vital (IIV). IIV merupakan sekumpulan infrastruktur strategis dan memiliki dampak yang besar apabila terjadi gangguan. National Security Operation Center (NSOC) merupakan pusat operasi keamanan siber lingkup nasional yang memiliki fungsi untuk memberikan layanan keamanan siber bagi IIV. Di Indonesia, IIV memiliki tingkat kerentanan dan ancaman siber yang tinggi, sementara langkah perbaikan mengenai kerentanan dan ancaman tersebut belum dilaksanakan dengan baik. Selain itu, belum terdapat kerangka kerja terkait pelaksanaan siklus pengelolaan kerentanan di NSOC untuk melindungi IIV. Penelitian ini bertujuan untuk mengusulkan National Security Operation Center-Vulnerability Management (NSOC-VM) sebagai kerangka kerja yang dapat diterapkan oleh NSOC untuk melakukan manajemen kerentanan. Kerangka kerja disusun berdasarkan siklus manajemen kerentanan dan diberikan rekomendasi penerapan menggunakan beberapa standar. Validasi kerangka kerja dilakukan menggunakan metode Expert Judgement dan dilakukan oleh pakar di bidang pelindungan IIV, pelaksanaan NSOC, dan manajemen kerentanan. Berdasarkan hasil penelitian, kerangka kerja NSOC-VM memiliki 5 tahapan, 10 aktivitas, dan 35 rekomendasi penerapan. Penilaian kuantitatif menggunakan Free-Marginal Multirater Kappa menunjukkan nilai Kappa sebesar 0.954 yang berarti usulan rekomendasi implementasi kerangka kerja mendapatkan kesepakatan para Expert Judgement pada level almost perfect agreement. Kerangka kerja ini diharapkan dapat diterapkan di NSOC untuk memberikan pelindungan pada IIV di Indonesia.

.....Cyber security is an essential aspect of Critical Information Infrastructure (CII). CII is a collection of strategic infrastructure and has a significant impact if disruptions occur. The National Security Operation Center (NSOC) is a national cyber Security Operation Center in Indonesia that provides CII with cyber security services. In Indonesia, CII has a high level of vulnerability and cyber threats. At the same time, remedial measures regarding these vulnerabilities and threats have not been appropriately implemented. In addition, there is also no framework for carrying out a vulnerability management cycle for NSOC to protect CII. This research proposes the National Security Operation Center-Vulnerability Management (NSOC-VM) Framework that NSOC can apply to manage vulnerability. The framework is designed based on the vulnerability management cycle and recommendations for implementation are given using several standards. The Framework validation was conducted using Expert Judgement in CII protection, SOC best practices, and vulnerability management implementation. Based on the result, the NSOC-VM Framework consists of 5 phases, 10 activities, and 35 practical recommendations. Quantitative research using Free-Marginal Multirater Kappa shows a kappa value of 0.954, which means that the proposed recommendations for implementing the Framework received agreement from expert judgment at almost perfect agreement level. It is hoped that this framework can be implemented in NSOC to provide CII protection in Indonesia.