Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) p-ISSN: 2355-7699
Vol. 12, No. 6, Desember 2025, hlm. 1291-1302 e-ISSN: 2528-6579

NSOC-VM: KERANGKA KERJA MANAJEMEN KERENTANAN PADA NATIONAL SECURITY OPERATION CENTER

Muhammad Azza Ulin Nuha*[1], Susila Windarta[2], Muhammad Salman[3]

[1,3]Universitas Indonesia, Depok, [2]Politeknik Siber dan Sandi Negara, Bogor
Email: [1]muhammad.azza21@ui.ac.id, [2]susila.windarta@poltekssn.ac.id, [3]muhammad.salman@ui.ac.id
*Penulis Korespondensi

(Naskah masuk: 31 Oktober 2024, diterima untuk diterbitkan: 09 Desember 2025)

Abstrak

Keamanan siber merupakan aspek penting dalam penyelenggaraan Infrastruktur Informasi Vital (IIV), yaitu sekumpulan infrastruktur strategis yang berdampak signifikan apabila mengalami gangguan. *National Security Operation Center* (NSOC) berperan sebagai pusat operasi keamanan siber nasional yang memberikan layanan keamanan bagi IIV. Di Indonesia, IIV menghadapi tingkat kerentanan dan ancaman siber yang tinggi, sementara pengelolaan kerentanannya masih menghadapi berbagai tantangan. Saat ini, belum tersedia kerangka kerja khusus yang mengatur pelaksanaan siklus manajemen kerentanan di NSOC untuk pelindungan IIV. Penelitian ini bertujuan untuk mengusulkan kerangka kerja *National Security Operation Center-Vulnerability Management* (NSOC-VM) yang dirancang untuk membantu NSOC dalam melakukan pengelolaan kerentanan. Kerangka kerja ini disusun dengan pendekatan *Plan-Do-Check-Act* (PDCA) dan dilengkapi dengan rekomendasi penerapan berdasarkan beberapa standar keamanan siber. Validasi dilakukan oleh sepuluh pakar yang memiliki keahlian dalam pelindungan IIV, operasional NSOC, dan manajemen kerentanan. Hasil penelitian menunjukkan bahwa kerangka kerja terdiri atas empat tahapan, sepuluh aktivitas utama, dan tiga puluh lima rekomendasi implementasi. Berdasarkan validasi yang dilakukan, kerangka kerja tersebut disetujui oleh para pakar sehingga dapat diterapkan oleh NSOC dalam mendukung pelindungan IIV di Indonesia.

Kata kunci: *IIV, NSOC, manajemen kerentanan, NSOC-VM, metode PDCA.*

NSOC-VM: A VULNERABILITY MANAGEMENT FRAMEWORK FOR NATIONAL SECURITY OPERATION CENTER

Abstract

Cybersecurity plays a pivotal role in safeguarding Critical Information Infrastructure (CII), which comprises strategic assets whose disruption could significantly impact national stability. The National Security Operation Center (NSOC) serves as Indonesia's central entity for cybersecurity operations, providing protection and response capabilities for CII. However, CII in Indonesia continues to face high levels of cyber threats and vulnerabilities, while the implementation of comprehensive vulnerability management practices remains limited. Furthermore, a dedicated framework governing the vulnerability management lifecycle within the NSOC context has yet to be established. This study proposes the National Security Operation Center–Vulnerability Management (NSOC-VM) framework to enhance the effectiveness of vulnerability management activities at the NSOC. The framework is structured using the Plan-Do-Check-Act (PDCA) methodology and incorporates implementation recommendations aligned with recognized cybersecurity standards. Validation was carried out through expert judgment involving ten professionals with expertise in CII protection, NSOC operations, and vulnerability management. The validated framework consists of four phases, ten key activities, and thirty-five implementation recommendations. The experts confirmed the framework's applicability and relevance, indicating its potential to support NSOC operations in strengthening CII protection in Indonesia.

Keywords: *CII, NSOC, vulnerability management, NSOC-VM, PDCA methods.*

1. PENDAHULUAN

Perkembangan teknologi pada masa kini sangat erat kaitannya dengan urgensi pelindungan *critical information infrastructure* atau Infrastruktur Informasi Vital (IIV). IIV merupakan infrastruktur yang penting untuk menunjang kebutuhan, kesehatan, keamanan, perekonomian, dan sosial masyarakat yang berdampak sangat besar apabila terjadi gangguan pada sektor dan proses di dalamnya

(Beckvard, 2022). Secara umum terdapat 8 sektor IIV di Indonesia yaitu sektor pemerintahan, energi dan sumber daya mineral, transportasi, keuangan, kesehatan, TIK, pangan, dan pertahanan (Presiden Republik Indonesia, 2022a; Putro & Sensuse, 2021)

Dalam operasional IIV, terdapat banyak risiko yang muncul dari sisi fisik infrastruktur, ruang siber, dan manusia yang mengoperasikannya (Homeland Security, 2013). Serangan siber menduduki peringkat kelima sebagai risiko yang dihadapi secara global pada tahun 2024 dan berdampak pada kelangsungan dan keamanan IIV (WEF, 2024). Diperlukan peran organisasi di bidang keamanan siber untuk melindungi IIV untuk memastikan aspek kerahasiaan, integritas, dan ketersediaan dapat terjaga dengan baik (Roshanaei, 2021).

Dalam memberikan pelindungan pada IIV, diperlukan adanya tim yang bertanggungjawab dan memiliki proses bisnis untuk memberikan layanan pengamanan. *Security Operation Center* (SOC) merupakan sebuah tim yang dapat memberikan pengamanan dan pertahanan pada IIV (Han dkk., 2019). Dalam rangka pelindungan IIV di Indonesia, *National* SOC (NSOC) merupakan SOC dalam lingkup nasional yang memiliki peran untuk memberikan layanan operasional keamanan siber untuk IIV. Dalam praktiknya, SOC dapat melakukan pengamanan dengan melibatkan kolaborasi antara *people, process,* dan *technology* (Vielberth dkk., 2020). SOC juga memiliki peran penting untuk melakukan berbagai fungsi seperti mendeteksi; melakukan penelusuran ancaman dan kerentanan lebih dalam; dan melaporkan adanya aktivitas mencurigakan (Mutemwa dkk., 2018).

Di Indonesia, celah kerentanan dan ancaman siber memiliki jumlah dan intensitas tinggi seperti insiden siber, kebocoran data, serangan pengubahan tampilan aplikasi *(defacement)*, aduan siber, dan temuan kerentanan melalui kegiatan uji penetrasi (BSSN, 2023). Kerentanan yang bersifat kritis ditemukan pada sistem elektronik lingkup pemerintahan seperti SQL *Injection* dan *Cross-site Scripting* (Darojat dkk., 2022; Setiawan dkk., 2023). Kerentanan yang ditemukan pada *website* milik pemerintah juga mengalami peningkatan sebesar 12% dari tahun 2018 hingga 2020 (Suyitno dkk., 2021). Namun, banyaknya kerentanan tersebut belum diimbangi dengan perbaikan kerentanan dengan baik seperti masih maraknya penggunaan perangkat lunak usang dan kata sandi yang lemah.

Berdasarkan kondisi tersebut, manajemen kerentanan diperlukan untuk menangani dan mengelola celah kerentanan dan ancaman siber IIV di Indonesia. Manajemen terhadap kerentanan dan ancaman siber yang baik diperlukan untuk mengurangi risiko dan dampaknya terhadap sistem elektronik (Magnussen dkk., 2023). Penerapan manajemen kerentanan pada IIV merupakan langkah penting berkaitan dengan nilai aset dan informasi di dalamnya (Mehri dkk., 2022). Manajemen kerentanan pada IIV di Indonesia dapat dilakukan oleh NSOC. Namun, untuk melaksanakan praktik manajemen kerentanan, belum terdapat panduan khusus yang dirancang dan dapat diimplementasikan oleh NSOC yang selaras dengan peran dan fungsi yang dimilikinya. Penelitian-penelitian sebelumnya berfokus pada penerapan di sektor tertentu dan belum terdapat integrasi dengan SOC terutama dalam rangka mendukung pelindungan pada IIV.

Pada penelitian ini, dilakukan perancangan kerangka kerja manajemen kerentanan pada NSOC untuk memberikan pelindungan pada IIV. Kerangka kerja ini diberi nama *National Security Operation Center-Vulnerability Management* (NSOC-VM). Kerangka kerja ini disusun dengan mengacu pada beberapa standar terkait manajemen kerentanan dan praktik terbaik pelaksanaan SOC untuk mendukung penerapan kerangka kerja tersebut. Hasil kerangka kerja tersebut divalidasi oleh para pakar internal NSOC berdasarkan kriteria tertentu untuk mendapatkan persetujuan dan perbaikan sehingga kerangka kerja tersebut dapat diterapkan oleh NSOC untuk melindungi IIV di Indonesia.

2. PENELITIAN TERKAIT

2.1. Manajemen Kerentanan

Manajemen kerentanan merupakan proses kerja yang penting untuk memastikan keamanan aset elektronik. Terdapat beberapa standar yang dapat diacu terkait manajemen kerentanan, yaitu ISO 27002:2022 (ISO, 2022), SANS - *Implementing a Vulnerability Management Process* (Palmaers, 2021), CISA - *Vulnerability Management Version 1.1* (CISA, 2016), NIST SP 800-53 r5 (NIST, 2020) dan NIST SP 800-40 (Souppaya & Scarfone, 2022). CISA, SANS, dan NIST SP 800-40 r4 memberikan penjelasan mengenai tahapan dan pelaksanaan manajemen kerentanan. Sedangkan ISO 27002 dan NIST SP 800-53 r5 memiliki daftar kontrol dan rekomendasi yang dapat diterapkan dalam lingkup keamanan informasi termasuk dalam pelaksanaan manajemen kerentanan. Dalam siklus manajemen kerentanan, NIST SP 800-40 r4 memiliki tahapan yang paling lengkap mencakup identifikasi aset hingga verifikasi perbaikan kerentanan. Selain itu, NIST SP 800-40 r4 juga merupakan versi terbaru yang dirilis pada tahun 2022, yaitu NIST SP 800-40 r4 - *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology.*

Pelaksanaan manajemen kerentanan telah diterapkan pada beberapa sektor IIV. Nikolaou dkk melakukan penelitian terkait manajemen insiden, identifikasi, dan pertukaran informasi kerentanan pada sektor energi (Nikolaou dkk., 2023). Sotiropoulos dkk memberikan usulan langkah manajemen kerentanan pada lingkup *Cyber Physical System* (CPS) (Sotiropoulos dkk., 2023). Chillar & Shrivastava melakukan penelitian terkait manajemen dan penilaian kerentanan pada sektor akademik

(Chhillar & Shrivastava, 2021). Avadanei dkk melakukan penelitian terkait pengembangan perangkat lunak manajemen kerentanan untuk sektor telekomunikasi (Avadanei dkk., 2021). Li dkk mengembangkan penilaian risiko kerentanan dan platform untuk manajemen kerentanan pada sektor transportasi (Li dkk., 2023). Berdasarkan kondisi tersebut, belum terdapat kerangka kerja manajemen kerentanan yang dapat diacu oleh SOC sesuai dengan fungsi yang beragam di dalamnya seperti pengawasan dan respons insiden keamanan siber yang beroperasi secara terus menerus serta memiliki berbagai tim dengan peran dan fungsi masing-masing. Kondisi yang terdapat dalam NSOC memerlukan manajemen kerentanan yang dinamis, komprehensif, dan kolaboratif sehingga dalam rangka pelindungan IIV di Indonesia, perlu adanya kerangka kerja manajemen kerentanan khusus yang dapat diacu oleh NSOC.

2.2. National Security Operation Center

IIV merupakan obyek yang menjadi prioritas tertinggi untuk dilakukan pengamanan dalam dunia siber (You dkk., 2024). Pelindungan pada IIV memerlukan beragam cara pengamanan seperti identifikasi kerentanan, pemantauan keamanan, dan pengamanan pada teknologi yang digunakan (Becker dkk., 2024). Langkah-langkah pelindungan IIV tersebut dapat dilakukan oleh SOC. Di Indonesia, peraturan terkait pelindungan IIV dijelaskan dalam Peraturan Presiden No. 82 tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Presiden Republik Indonesia, 2022a). Dalam peraturan tersebut, Badan Siber dan Sandi Negara (BSSN) berperan dalam penyusunan kerangka kerja pelindungan IIV. Oleh karena itu, disusun Peraturan BSSN No. 8 tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital yang memberikan pedoman dan acuan tentang pelindungan IIV.

Manajemen kerentanan merupakan salah satu bentuk penerapan kerangka kerja pelindungan IIV yang dapat dilakukan oleh NSOC sebagai bagian dari BSSN dan SOC lingkup nasional yang memiliki kapabilitas operasional keamanan siber. Penelitian terkait kerangka kerja manajemen kerentanan pada SOC telah diusulkan oleh Hore dkk untuk melindungi aset yang dikelolanya (Hore dkk., 2023). Farris dkk juga mengusulkan kerangka kerja manajemen dan penentuan prioritas kerentanan berdasarkan hasil pemantauan aset SOC (Farris dkk., 2018). Namun, penelitian tersebut hanya terbatas dilakukan untuk melindungi aset internal NSOC. Pada penelitian ini, NSOC-VM dirancang untuk dapat diterapkan NSOC dalam melindungi aset IIV secara menyeluruh.

NSOC terdiri atas sembilan tim yang menjalankan tugas dan fungsi masing-masing sebagaimana dijelaskan pada Tabel 1. Tugas dan fungsi ini terdapat dalam *Grand Design* NSOC (Pusat Operasi Keamanan Siber Nasional, 2021) dan Keputusan Kepala BSSN No. 248 tahun 2022 tentang Peta Proses Bisnis Badan Siber dan Sandi Negara (BSSN, 2022).

Tabel 1. Tugas dan fungsi tim dalam NSOC

No	Nama Tim	Tugas dan Fungsi
1.	Monitoring	• Monitoring dan penyusunan laporan anomali trafik berdasarkan sistem monitoring pada jaringan publik dan *stakeholder* • Pelaporan *situational awareness* • Dokumentasi aset informasi
2.	*Cyber Threat Intelligence* (CTI)	• Monitoring kebocoran data dan ancaman siber • Pengolahan informasi kebocoran data melalui *threat intelligence platform* • Pengumpulan informasi dan ancaman siber berupa *threat actor* dan APT
3.	IT *Security Assessment* (ITSA)	• Penilaian risiko berdasarkan kerentanan yang ditemukan, kemungkinan eksploitasi, dan dampak yang ditimbulkan • Pengujian kerentanan dan pemberian rekomendasi perbaikan secara umum
4.	Proteksi	• Asistensi proteksi perbaikan kerentanan pada sistem • Verifikasi perbaikan sistem setelah pelaksanaan pengujian • Pemasangan, pemantauan, analisis, validasi ancaman pada sensor berbasis *endpoint* • Menyusun imbauan keamanan • Melakukan *hardening* pada sistem
5.	Infrastruktur	• Pemantauan terhadap pelaksanaan dan kinerja infrastruktur TI • Perencanaan, pengelolaan, dan evaluasi pada infrastruktur TI • Pengelolaan pada seluruh fasilitas dan aset
6.	*Threat Hunting*	• Penelusuran potensi ancaman siber • Penelusuran indikasi kerentanan pada aset • Pengembangan, pemasangan, dan manajemen terhadap sensor monitoring berbasis open-source.
7.	Respon Insiden	• Pemberian peringatan dini terkait ancaman siber • Pertukaran informasi terenkripsi dan *lesson learned* dari insiden siber
8.	Forensik Digital	• Memberikan dukungan penyidikan • Pemeriksaan forensik digital • Perbantuan tenaga ahli
9.	Analisis *Malware*	• Penyusunan dokumen analisis *Malware* • Pengembangan layanan *honeynet* • Pemasangan dan analisis terhadap perangkat *honeypot*

Dalam menjalankan tugas dan fungsi tersebut, NSOC mengacu pada standar dan praktik terbaik terkait pelaksanaan SOC, diantaranya adalah NIST *Cybersecurity Framework* (NIST, 2024) dan MITRE SOC *Framework* (Knerler dkk., 2022). MITRE SOC *Framework* digunakan sebagai acuan karena memiliki uraian lengkap tentang pelaksanaan SOC berupa bentuk, fungsi, dan strategi SOC dalam menjalankan tiap fungsi tersebut sesuai kebutuhan pelindungan IIV serta dapat diterapkan secara langsung oleh tim dalam NSOC sesuai dengan tugas dan fungsi masing-masing.

3. METODE PENELITIAN

3.1. Studi Literatur dan Wawancara

Pada tahap studi literatur, dilakukan penelitian secara mendalam terhadap standar terkait manajemen kerentanan. Standar terkait manajemen kerentanan yang digunakan adalah NIST SP 800-40 r4 – *Guide to Enterprise Patch Management Planning* karena memiliki tahapan manajemen kerentanan yang lengkap dan merupakan versi yang terbaru. Panduan ini memiliki tiga tahapan manajemen kerentanan, yaitu,

1) Mengetahui Kerentanan pada Aset
   - Melakukan inventarisasi aset TI
   - Melakukan pemantauan kerentanan pada aset TI
2) Merencanakan Respons Kerentanan
   - Melakukan penilaian risiko berdasarkan kerentanan pada aset
   - Menentukan bentuk respons risiko
   - Merumuskan cara untuk merespons risiko
3) Melaksanakan Respons Kerentanan
   - Menyiapkan respons
   - Menerapkan respons
   - Melakukan verifikasi pada respons
   - Melakukan pemantauan respons

Tahap wawancara dilakukan terhadap Kepala NSOC BSSN untuk mendapatkan data primer penelitian. Wawancara dilakukan secara verbal dan hasilnya dikonversi ke dalam bentuk teks untuk dianalisis. Poin-poin utama pertanyaan wawancara tersebut meliputi: (1) Standar yang diacu oleh NSOC dalam menjalankan tugas dan fungsinya (2) Urgensi manajemen kerentanan bagi NSOC sebagai bentuk pelindungan terhadap IIV (3) Panduan terkait manajemen kerentanan bagi NSOC (4) Tim dalam NSOC yang relevan terhadap pelaksanaan manajemen kerentanan.

Berdasarkan hasil wawancara, diperoleh informasi bahwa NSOC mengacu pada praktik terbaik SOC dalam MITRE SOC *Framework*. Manajemen kerentanan penting untuk diterapkan pada NSOC untuk mendukung penyusunan dan penerapan kerangka kerja pelindungan IIV. Dalam pelaksanaan manajemen kerentanan, NSOC belum memiliki panduan yang dapat diacu sehingga diperlukan penyusunan kerangka kerja manajemen kerentanan yang dapat diterapkan oleh NSOC. Selain itu, terdapat 6 tim yang memiliki tugas dan fungsi utama yang relevan dengan pelaksanaan manajemen kerentanan, yaitu tim Monitoring, CTI, ITSA, Proteksi, *Threat Hunting*, dan Respon Insiden. Tim lain yaitu tim Infrastruktur, Forensik Digital, dan Analisis *Malware* dapat berperan sebagai tim pendukung dalam pelaksanaan manajemen kerentanan apabila dibutuhkan tindakan lebih lanjut.

3.2. Perancangan Kerangka Kerja

Tahap ini dilakukan dengan merancang kerangka kerja NSOC-VM. Perancangan ini diperlukan karena belum adanya kerangka kerja khusus untuk praktik manajemen kerentanan pada NSOC yang sesuai dengan fungsi, tim, dan operasional di dalamnya.

Dalam perancangan NSOC-VM, terdapat dua referensi utama yang dilakukan sintesis, yaitu NIST SP 800-40 dan MITRE SOC *Framework.* NIST SP 800-40 digunakan sebagai referensi tahapan siklus manajemen kerentanan secara menyeluruh dimulai dari identifikasi aset hingga pemantauan. Sedangkan MITRE SOC *Framework* digunakan sebagai referensi mengenai fungsi dan pembagian wewenang tim dalam NSOC. Hasil sintesis ini akan dipetakan ke dalam aktivitas siklus NSOC-VM. Hasil pemetaan aktivitas ini disusun menggunakan metode *Plan-Do-Check-Act* (PDCA) untuk menggambarkan siklus manajemen kerentanan secara komprehensif. PDCA digunakan untuk menggambarkan siklus berulang dan agar dapat dilakukan evaluasi secara berkala sesuai kebutuhan peningkatan NSOC. Siklus NSOC-VM tersebut diberikan rekomendasi penerapan berdasarkan standar-standar yang relevan dalam penerapan rekomendasi keamanan informasi dan manajemen kerentanan. Oleh karena itu, kerangka kerja yang dihasilkan dapat menjadi rujukan dalam pelaksanaan manajemen kerentanan pada NSOC untuk melindungi IIV dengan langkah-langkah manajemen kerentanan yang lengkap dan sesuai dengan fungsi yang didukung NSOC.

3.3. Validasi Kerangka Kerja

Setelah dilakukan penyusunan kerangka kerja dan pemberian rekomendasi penerapan, selanjutnya dilakukan validasi terhadap rancangan NSOC-VM. Terdapat penelitian lain yang menggunakan validasi terhadap hasil rancangan kerangka kerja terkait keamanan siber. Sensuse dkk melakukan validasi rancangan kerangka kerja keamanan siber untuk Ibu Kota Nusantara (IKN) terhadap tiga pakar yang memiliki pengalaman dan kompetensi terkait keamanan siber dalam sektor pemerintahan (Sensuse dkk., 2022). Aferudin & Ramli melakukan validasi kerangka kerja berbagi informasi keamanan siber terhadap tiga pakar di bidang keamanan siber dan pelindungan IIV (Aferudin & Ramli, 2022). Pada penelitian ini, validasi dilakukan oleh para pakar di NSOC yang memenuhi beberapa kriteria tertentu, yaitu (1) Aktif bekerja dan memiliki pengalaman kerja minimal lima tahun (2) Memiliki pemahaman terkait pelindungan IIV, pelaksanaan NSOC, dan/atau manajemen kerentanan (3) Memiliki kompetensi terkait fungsi SOC. Validasi ini dilakukan untuk mendapatkan persetujuan, saran, dan perbaikan pada NSOC-VM sehingga dapat diterapkan oleh NSOC dalam memberikan pelindungan pada IIV.

4. HASIL DAN PEMBAHASAN

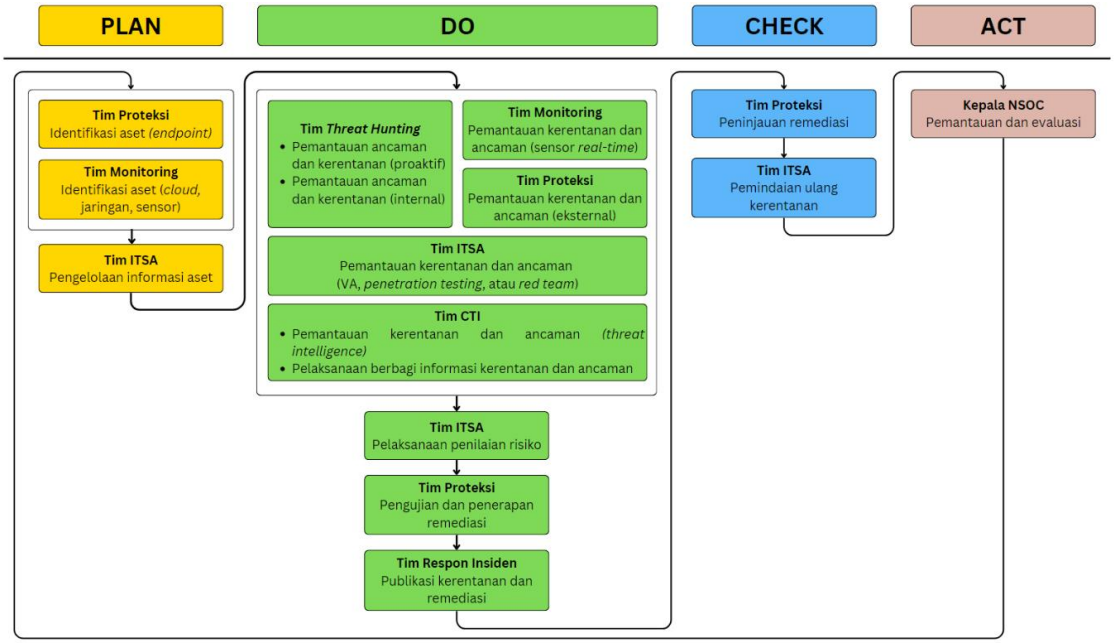
4.1. Pemetaan Aktivitas

Komponen aktivitas NSOC-VM disusun berdasarkan dua standar utama, yaitu NIST SP 800-40 r4 dan MITRE SOC *Framework*. Langkah-langkah NSOC-VM disusun berdasarkan tahapan manajemen kerentanan pada NIST SP 800-40 r4 dan kategori fungsi SOC dalam MITRE SOC *Framework*. Hasil pemetaan tersebut dilakukan generalisasi terhadap tugas dan fungsi masing-masing tim dalam SOC yang dijelaskan dalam Tabel 3.

Tabel 3. Pemetaan Aktivitas NSOC-VM

NIST SP 800-40 r4	MITRE SOC *Framework*	Generalisasi
Melakukan inventarisasi aset TI	Merekayasa, menerapkan, mengoperasikan, dan memelihara deteksi dan proteksi *endpoint*	Identifikasi aset *(endpoint)*
	Merekayasa, menerapkan, mengoperasikan, dan memelihara deteksi dan proteksi untuk perangkat seluler	
	Merekayasa, menerapkan, mengoperasikan, dan memelihara deteksi dan proteksi *cloud*	Identifikasi aset (*cloud*, jaringan, sensor, teknologi operasional (OT))
	Merekayasa, menerapkan, mengoperasikan, dan memelihara infrastruktur keamanan jaringan	
	Merekayasa, menerapkan, mengoperasikan, dan memelihara platform SIEM, SOAR, CTI, UEBA, *Big Data*, dan teknologi lainnya.	
	Merekayasa, menerapkan, mengoperasikan, dan memelihara kemampuan deteksi dan pelindungan siber untuk teknologi operasional	
	Mengidentifikasi dan mendokumentasikan semua aset TI.	Pengelolaan informasi aset
Melakukan pemantauan kerentanan pada aset TI	Mengumpulkan dan memproses informasi ancaman siber (CTI) Menganalisis tren dan TTP dari pelaku ancaman siber	Pemantauan kerentanan dan ancaman (*threat intelligence)*
	Mencari potensi ancaman di luar cakupan perangkat deteksi	Pemantauan ancaman dan kerentanan (proaktif)
	Melakukan *triage* dan analisis ancaman siber dari notifikasi ancaman secara *real-time*	Pemantauan kerentanan dan ancaman (sensor *real-time*)
	Memberikan dukungan deteksi ancaman dari sumber internal	Pemantauan ancaman dan kerentanan (internal)
	Mengelola laporan kerentanan dari peretas etis	Pemantauan kerentanan dan ancaman (eksternal)
	Mengidentifikasi kerentanan menggunakan *tools*	Pemantauan kerentanan dan ancaman (VA, *penetration testing*, atau *red team*)
	Mengidentifikasi kerentanan baru *(zero-day)*	
	Mengidentifikasi kerentanan melalui melalui uji penetrasi, *red teaming*, dan *purple teaming*	
	Membagikan informasi ancaman siber kepada pihak di luar SOC	Pelaksanaan berbagi informasi kerentanan dan ancaman
Merencanakan respons risiko	Mengevaluasi dampak kerentanan dan merekomendasikan tindakan mitigasi	Pelaksanaan penilaian risiko
Menyiapkan respons	Memperbaiki kerentanan melalui penerapan *patch* atau mitigasi risiko	Pengujian dan penerapan remediasi
Menerapkan respons	Menyusun dan mendistribusikan hasil analisis terkait aset, risiko, ancaman, insiden, dan kerentanan kepada pihak luar	Publikasi kerentanan dan remediasi
Melakukan verifikasi pada respons	Memperbaiki kerentanan melalui penerapan *patch* atau mitigasi risiko	Peninjauan remediasi
	Mengidentifikasi kerentanan menggunakan *tools* identifikasi kerentanan	Pemindaian ulang kerentanan
Memantau respons	Membuat dan mengevaluasi rencana yang dirancang	Pemantauan dan evaluasi

Berdasarkan pemetaan aktivitas pada Tabel 3, terdapat tujuh langkah manajemen kerentanan pada NIST SP 800-40 r4 yang dipetakan sesuai fungsi SOC dalam MITRE SOC *Framework.* Hasil pemetaan aktivitas tersebut dapat dilakukan oleh NSOC untuk melakukan tahapan NSOC-VM. Masing-masing aktivitas tersebut dapat dijelaskan dan dikorelasikan terhadap tugas dan fungsi tim dalam NSOC sebagaimana dijelaskan dalam Tabel 1. Tahapan manajemen kerentanan dapat disusun menggunakan metode PDCA untuk menggambarkan siklus NSOC-VM. Siklus NSOC-VM yang dirancang ditunjukkan pada Gambar 1 dan memiliki penjelasan sebagai berikut,



Gambar 1. Siklus Kerangka Kerja NSOC-VM

a) Identifikasi Aset
Aktivitas pertama adalah identifikasi aset, yaitu aset *endpoint, cloud*, jaringan, sensor, dan teknologi operasional (OT). Pada NSOC, aktivitas tersebut dilakukan oleh tim Proteksi dan tim Monitoring, Tim Proteksi memiliki fungsi untuk pemasangan dan pengelolaan sensor keamanan berbasis *endpoint* yang dapat digunakan untuk identifikasi aset *endpoint*. Sedangkan identifikasi aset *cloud*, jaringan, sensor, dan teknologi operasional (OT) dapat dilakukan oleh Tim Monitoring melalui sistem *monitoring* jaringan yang dikelolanya. Identifikasi aset ini dilakukan dengan mengambil informasi konfigurasi dasar dari aset seperti spesifikasi aset, pemilik aset, layanan yang berjalan, dan informasi lain dari aset yang penting untuk diidentifikasi.

b) Pengelolaan Informasi Aset
Setelah informasi terkait aset dapat diidentifikasi, aktivitas pengelolaan informasi aset dilakukan dengan membuat basis data informasi aset, penentuan prioritas, dan pengelompokan aset yang memiliki level prioritas yang sama (Swanson dkk., 2006). Aktivitas ini dilakukan oleh Tim ITSA untuk digunakan dalam penilaian risiko kerentanan pada aset sesuai fungsinya dalam melakukan penilaian kerentanan.

c) Pemantauan Kerentanan dan Ancaman
Aktivitas pemantauan kerentanan dan ancaman dilakukan oleh beberapa tim sesuai tugas dan fungsinya, yaitu Tim CTI, *Threat Hunting*, Monitoring, Proteksi, dan ITSA. Tim CTI berperan dalam pelaksanaan siklus *threat intelligence* (Recorded Future, 2022), Tim *Threat Hunting* melakukan penelusuran ancaman proaktif melalui sumber terbuka dan melaksanakan deteksi ancaman dari internal (CISA, 2020), Tim Monitoring melakukan pemantauan melalui sistem *monitoring* jaringan untuk mendapatkan hasil pemantauan secara *real-time,* Tim Proteksi berperan dalam penyelenggaraan *vulnerability disclosure program* (ISO, 2018), dan Tim ITSA berperan dalam pengujian kerentanan pada aset melalui VA, *Penetration Testing,* atau *Red Team*.

d) Pelaksanaan berbagi informasi kerentanan dan ancaman
Aktivitas ini dilakukan oleh Tim CTI melalui platform *threat intelligence* yang dikelolanya. Aktivitas ini berfungsi untuk peningkatan strategi keamanan siber yang terkoordinasi satu sama lain ketika terdapat kerentanan dan ancaman baru yang ditemukan. CTI dapat menyelenggarakan berbagi informasi dengan sektor IIV dengan mengacu pada standar berbagi informasi keamanan siber seperti NIST SP 800-150 (Johnson dkk., 2016) dan ENISA-ISAC (ENISA, 2020).

e) Pelaksanaan Penilaian Risiko
Aktivitas penilaian risiko dilaksanakan oleh Tim ITSA berdasarkan kerentanan dan ancaman yang ditemukan pada aset. Penilaian risiko dilakukan berdasarkan kemungkinan terjadi, dampak, dan respons terhadap risiko yang akan diterapkan sesuai nilainya (NIST, 2012). Kerentanan dan ancaman dengan nilai risiko tinggi diprioritaskan untuk segera diberikan respons penanganan. Penanganan yang diberikan dapat berupa *accept, mitigate, transfer,* atau *avoid* terhadap risiko sesuai dengan keputusan.

f) Pengujian dan Penerapan Remediasi
Aktivitas pengujian dan penerapan remediasi dilaksanakan oleh Tim Proteksi melalui fungsi asistensi. Berdasarkan hasil penilaian risiko, aktivitas ini dilakukan dengan menerapkan respons risiko yang ditentukan. Respons ini dapat

Tabel 4. Pembandingan kerangka kerja manajemen kerentanan

Perbandingan Penelitian	(Sotiropoulos dkk., 2023)	(Chhillar & Shrivastava, 2021)	(Avadanei dkk., 2021)	(Li dkk., 2023)	(Nikolaou dkk., 2023)	(Hore dkk., 2023)	NSOC-VM *Framework*
Sektor	CPS	Akademik	Telekomunikasi	Transportasi	Energi	CSOC	IIV
Pelaksana	Pengembang aplikasi	Pengelola TI	Operator telekomunikasi	Operator jaringan	Operator energi	Tim Keamanan CSOC	NSOC
Identifikasi aset	✓	✓	×	✓	×	✓	✓
Pengelolaan informasi aset	✓	×	×	✓	✓	×	✓
Pemantauan kerentanan	✓	✓	✓	✓	✓	✓	✓
Berbagi informasi kerentanan dan ancaman	×	×	✓	×	✓	×	✓
Penilaian risiko	✓	✓	✓	✓	✓	✓	✓
Pengujian dan penerapan remediasi	×	✓	×	✓	×	✓	✓
Publikasi kerentanan dan remediasi	×	×	✓	×	×	×	✓
Peninjauan remediasi	×	×	×	✓	×	×	✓
Pemindaian ulang kerentanan	×	×	×	✓	×	×	✓
Pemantauan dan evaluasi	✓	×	×	✓	✓	✓	✓

dilakukan berupa penerapan *patching* dan remediasi. Apabila respons yang dihasilkan berupa *patching,* dilakukan pengujian terhadap *patch* untuk memastikan *patch* tersebut dapat digunakan dengan aman, terhindar dari *malware,* dan tidak mengganggu proses lain yang berjalan. *Patch* yang berhasil diuji akan diinformasikan kepada pemilik aset yang terdampak. Apabila tidak terdapat *patch* yang tersedia, dilakukan langkah mitigasi non-*patching* untuk mengatasi risiko kerentanan tersebut dan diberikan panduan penerapannya (Souppaya & Scarfone, 2022).

g) Publikasi Kerentanan dan Remediasi
Aktivitas ini dilakukan oleh tim Respons Insiden melalui fungsinya untuk memberikan peringatan ancaman siber. Publikasi hasil pengujian dan penerapan remediasi berbentuk dokumen imbauan keamanan agar dapat dijadikan acuan oleh pemilik aset terdampak. Publikasi ini memuat informasi seperti jenis dan deskripsi kerentanan serta langkah penerapan *patch* dan remediasi yang dapat dilakukan. Publikasi ini dikategorisasi berdasarkan peruntukan informasi di dalamnya dan diberikan label klasifikasi tertentu (FIRST, 2022).

h) Peninjauan Remediasi
Aktivitas peninjauan dilakukan untuk memastikan remediasi telah diterapkan oleh pemilik aset dengan baik. Peninjauan ini dilakukan oleh Tim Proteksi melalui fungsi asistensi dan verifikasi serta disesuaikan dengan langkah remediasi yang telah dilakukan. Apabila dilakukan *patching,* peninjauan dilakukan untuk memastikan *patching* pada aset diimplementasikan dengan baik. Apabila diterapkan remediasi non-*patching,* peninjauan dilakukan untuk memastikan langkah non-*patching* dapat mengatasi kerentanan yang berdampak pada aset.

i) Pemindaian Ulang Kerentanan
Aktivitas pemindaian ulang kerentanan dilakukan oleh tim ITSA untuk memastikan celah kerentanan pada aset telah ditutup. Pemindaian ulang dapat dilakukan dengan *vulnerability assessment, penetration testing,* atau *red teaming* terhadap aset yang telah dilakukan perbaikan.

j) Pemantauan dan Evaluasi
Aktivitas pemantauan dan evaluasi merupakan langkah berkelanjutan yang dapat dilakukan oleh Kepala NSOC. Aktivitas ini diperlukan untuk memastikan pelaksanaan kerangka kerja dapat diterapkan dengan baik oleh tim-tim dalam NSOC yang terlibat. Selain itu, Kepala NSOC juga melakukan evaluasi untuk peningkatan kinerja dan peningkatan kompetensi dalam pelaksanaan manajemen kerentanan.

Tahapan dalam siklus NSOC-VM tersebut dapat dijadikan sebagai perbandingan terhadap penelitian sebelumnya terkait kerangka kerja manajemen

kerentanan pada beberapa sektor IIV. Berdasarkan Tabel 4, diperoleh informasi bahwa NSOC-VM memiliki aktivitas dan langkah yang lebih komprehensif dalam melaksanakan siklus manajemen kerentanan pada NSOC sesuai dengan fungsi-fungsi yang dijalankannya.

Pemetaan aktivitas dalam NSOC-VM dapat ditulis dalam bentuk kode yang merujuk pada tiap aktivitas sebagaimana dijelaskan dalam Tabel 5. Hasil pemetaan tersebut menunjukkan bahwa dari 10 aktivitas, terdapat 2 aktivitas yang dapat dilakukan pada tahap *Plan*, 5 aktivitas pada tahap *Do*, 2 aktivitas pada tahap *Check*, dan 1 aktivitas pada tahap *Act.*

Tabel 5. Kode Aktivitas NSOC-VM

Tahap	Aktivitas	Tim	Kode
Plan	Identifikasi aset	Proteksi Monitoring	PL-01
	Pengelolaan informasi aset	ITSA	PL-02
Do	Pemantauan kerentanan dan ancaman	*Threat Hunting* Proteksi Monitoring ITSA CTI	DO-01
	Pelaksanaan berbagi informasi kerentanan dan ancaman	CTI	DO-02
	Pelaksanaan penilaian risiko	ITSA	DO-03
	Pengujian dan penerapan remediasi	Proteksi	DO-04
	Publikasi kerentanan dan remediasi	Respon Insiden	DO-05
Check	Peninjauan remediasi	Proteksi	CH-01
	Pemindaian ulang kerentanan	ITSA	CH-02
Act	Pemantauan dan evaluasi	Kepala NSOC	AC-01

4.2. Rekomendasi Penerapan

Setelah dilakukan perancangan, selanjutnya dapat diberikan rekomendasi penerapan terhadap pelaksanaan NSOC-VM pada NSOC sesuai dengan beberapa panduan atau kontrol keamanan informasi, yaitu NIST SP 800-40 r4, ISO 27002:2022, NIST SP 800-53 r5, NIST SP 800-18, dan *Threat Intelligence Handbook*. Rekomendasi penerapan tersebut dapat diterapkan berdasarkan kode aktivitas pada Tabel 4 dan diberikan detail rekomendasi dan referensinya dalam Tabel 6.

Tabel 6. Rekomendasi Penerapan NSOC-VM

TAHAP *PLAN*			
Aktivitas	**No.**	**Rekomendasi**	**Referensi**
PL-01	1	Menyusun informasi nama aset disertai pemilik aset, diperbarui secara berkala, disimpan, dan dipertukarkan dengan aman	C.5.9 (ISO, 2022)
	2	Menyusun, mendokumentasikan, dan memperbarui informasi konfigurasi dasar dari aset	CM-2 (NIST, 2020) C.8.9 (ISO, 2022)
PL-02	3	Mengembangkan perencanaan berkelanjutan terkait skenario penanganan kerentanan	CP-2 (NIST, 2020) (Souppaya & Scarfone, 2022)
	4	Menyusun dan menerapkan strategi penanganan kerentanan pada aset, meninjau strategi secara berkala, dan memperbarui strategi tersebut sesuai dengan kebutuhan	PM-9 (NIST, 2020)
	5	Mengembangkan dan memperbarui sistem informasi aset secara berkala	PM-5 (NIST, 2020)
	6	Menyimpan informasi setiap aset ke dalam grup berdasarkan aspek *confidentiality, integrity,* dan *availability*	C.5.12 (ISO, 2022) (Souppaya & Scarfone, 2022)
TAHAP *DO*			
Aktivitas	**No.**	**Rekomendasi**	**Referensi**
DO-01	7	Menjalankan program deteksi *insider threat*	PM-12 (NIST, 2020)
	8	Menyelenggarakan pencarian indikator kompromi dan pencarian ancaman proaktif	RA-10 (NIST, 2020)
	9	Menerapkan identifikasi kode berbahaya pada aset untuk deteksi di sisi *endpoint*, memperbarui saat rilis baru tersedia, melakukan pemindaian berkala, dan mengirim hasil respons terhadap deteksi	SI-3 (NIST, 2020)
	10	Menyediakan saluran untuk penerimaan laporan kerentanan dari publik	RA-5 (NIST, 2020)
	11	Melakukan identifikasi dan pemantauan secara berkelanjutan ancaman dan kerentanan aset menggunakan *tools*, menganalisis anomali yang terdeteksi, dan penyesuaian ketika terjadi perubahan aset	SI-4, CA-7 (NIST, 2020) C.8.16 (ISO, 2022)
	12	Melakukan pemindaian kerentanan secara berkala dan ketika terdapat kerentanan baru yang muncul pada aset, menganalisis, dan melaporkan hasil pemindaian tersebut	RA-5 (NIST, 2020) C.8.29 (ISO, 2022)
	13	Menyelenggarakan uji penetrasi atau *red team* terhadap aset	CA-8 (NIST, 2020) C.8.29 (ISO, 2022)

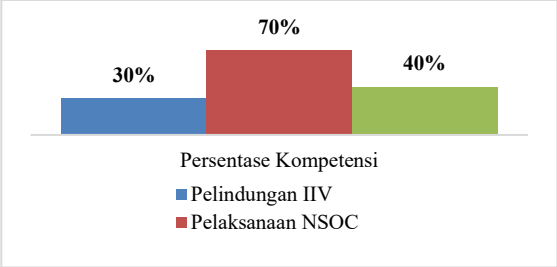
TAHAP *PLAN*			
DO-02	14	Melakukan pengumpulan, pemrosesan, analisis, dan pelaporan informasi intelijen	C.5.7 (ISO, 2022) (Recorded Future, 2022)
	15	Melaksanakan perencanaan, penerapan, dan evaluasi berbagi informasi kerentanan dan ancaman	PM-16 (NIST, 2020) (Johnson dkk., 2016)
	16	Menerapkan klasifikasi terhadap informasi kerentanan dan ancaman yang dipertukarkan	(Johnson dkk., 2016)
DO-03	17	Mengelola dan mendokumentasikan seluruh kerentanan yang ditemukan pada aset	C.8.8 (ISO, 2022)
	18	Melaksanakan penilaian risiko terhadap aset, menentukan kemungkinan dan dampak, serta mendokumentasikan hasil penilaian risiko	RA-3 (NIST, 2020)
	19	Menentukan respons risiko berdasarkan hasil penilaian risiko terhadap kerentanan dan ketentuan toleransi risiko yang ditetapkan	RA-7 (NIST, 2020)
	20	Memprioritaskan aset dengan nilai risiko yang tinggi untuk dilakukan penanganan	C.8.8 (ISO, 2022)
DO-04	21	Mengidentifikasi dan menguji perbaikan kerentanan atau pembaruan sistem aset sebelum dipasang untuk mengetahui efektivitas dan potensi dampak yang ditimbulkan	SI-2 (NIST, 2020)
	22	Mengidentifikasi, meninjau, dan mendokumentasikan perubahan pada aset berdasarkan hasil pengujian perbaikan	CM-3 (NIST, 2020)
	23	Menganalisis perubahan yang terjadi, memastikan perbaikan telah dilaksanakan dengan sesuai, dan mendapatkan hasil yang diharapkan	CM-4 (NIST, 2020)
	24	Melakukan *backup* sebelum melakukan percobaan pengujian perbaikan	C.8.13 (ISO, 2022)
DO-05	25	Melakukan diseminasi terhadap peringatan keamanan terkait kerentanan dan ancaman, perbaikannya, serta rekomendasi perbaikan kepada pihak luar sesuai prosedur yang digunakan	SI-5 (NIST, 2020) C.5.24 (ISO, 2022)
	26	Menerapkan kebijakan pelindungan informasi sensitif yang dipublikasikan	PM-17 (NIST, 2020)
	27	Mengirimkan informasi kerentanan dan remediasinya kepada pihak yang tepat	IR-6 (NIST, 2020) C.5.8 (ISO, 2022)
TAHAP *CHECK*			
Aktivitas	**No.**	**Rekomendasi**	**Referensi**
CH-01	28	Meninjau penerapan remediasi yang dilakukan	CA-5 (NIST, 2020)
	29	Mendokumentasikan log atau bukti remediasi kerentanan dan ancaman	C.8.15 (ISO, 2022)
CH-02	30	Melakukan pemindaian kerentanan, uji penetrasi, atau pengujian ulang terhadap aset yang telah dilakukan perbaikan	RA-5, CA-8 (NIST, 2020) C.8.29 (ISO, 2022)
TAHAP *ACT*			
Aktivitas	**No.**	**Rekomendasi**	**Referensi**
AC-01	31	Melakukan pemantauan berkelanjutan untuk memastikan remediasi kerentanan diterapkan	CA-7 (NIST, 2020) C.8.16 (ISO, 2022)
	32	Menganalisis, memantau, dan melaporkan hasil manajemen kerentanan untuk perbaikan dan peningkatan	PM-6 (NIST, 2020) C.5.27 (ISO, 2022)
	33	Mengevaluasi kepatuhan terhadap prosedur pelaksanaan manajemen kerentanan secara berkala	C.5.36 (ISO, 2022)
	34	Memperoleh umpan balik dari pihak lain untuk evaluasi	C.5.5 (ISO, 2022)
	35	Menyelenggarakan penguatan pelatihan kompetensi sesuai dengan tugas dan fungsi	AT-3 (NIST, 2020) C.6.3 (ISO, 2022)

4.3. Validasi

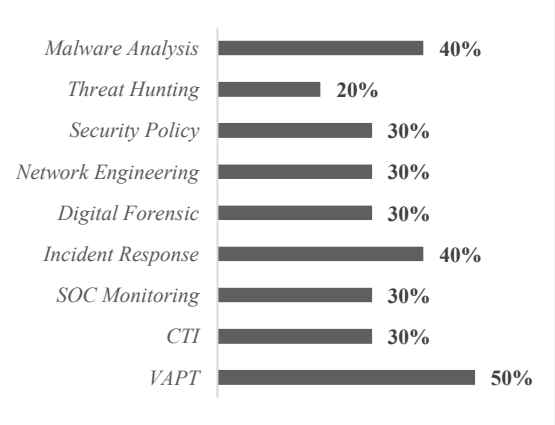
Pada tahap ini, dilakukan validasi terhadap rancangan NSOC-VM. Validasi dilakukan dengan wawancara terstruktur terhadap 10 pakar internal NSOC sebagai representasi keseluruhan tim dalam NSOC. Validasi ini dilakukan untuk mendapatkan persetujuan dan perbaikan dari usulan pelaksana NSOC-VM. Pemilihan pakar tersebut berdasarkan pada beberapa kriteria. Gambar 2 menunjukkan distribusi persentase kompetensi keseluruhan pakar secara umum terhadap pelindungan IIV, pelaksanaan NSOC, dan manajemen kerentanan. Pemilihan pakar juga dilakukan berdasarkan penguasaan fungsi SOC yang diterapkan dalam NSOC. Distribusi persentase keseluruhan pakar yang menguasai fungsi dalam NSOC digambarkan dalam Gambar 3.

Proses validasi dilakukan terhadap siklus dan rekomendasi penerapan NSOC-VM. Berdasarkan hasil validasi, keseluruhan pakar menyatakan setuju terhadap rancangan siklus NSOC-VM. Selain memberikan persetujuan, para pakar juga menyampaikan saran dan masukan terkait pelaksanaan dan penerapan NSOC-VM. Kerangka kerja diharapkan memiliki tujuan capaian yang jelas dan terukur serta dokumentasi pelaksanaan yang baik.

Saran ini dapat dipenuhi berdasarkan kebijakan dari Kepala NSOC BSSN terkait pelaksanaan manajemen kerentanan. Selain itu, diperlukan adanya panduan teknis untuk melakukan tiap aktivitas agar dapat menjalankan siklus manajemen kerentanan dengan sesuai dan dapat dipertanggungjawabkan. Panduan ini dapat disusun oleh masing-masing Tim sesuai dengan tugas dan fungsinya di NSOC.



Gambar 2. Distribusi kompetensi pakar secara umum



Gambar 3. Distribusi penguasaan pakar terhadap fungsi SOC

Pelaksanaan kerangka kerja juga harus didukung dengan komunikasi dan integrasi yang baik antar tim. Karena melibatkan sinergi banyak tim, pelaksanaan manajemen kerentanan tersebut dapat terorganisir dan terukur. Pelaksanaan tersebut dapat didukung dengan adanya aplikasi atau platform khusus manajemen kerentanan. Pelaksanaan manajemen kerentanan menggunakan aplikasi berbasis *website* telah diusulkan Russo dkk dan Li dkk pada sektor transportasi. Kedua penelitian tersebut memanfaatkan platform khusus untuk menjalankan kerangka kerja manajemen kerentanan sehingga dapat dilakukan otomatisasi, terstruktur, dan terintegrasi dengan berbagai dukungan perangkat lainnya (Li dkk., 2023; Russo dkk., 2019). Oleh karena itu, pemanfaatan platform juga dapat diterapkan pada kerangka kerja NSOC-VM. Platform tersebut juga harus terintegrasi dengan aplikasi lain yang telah dikelola oleh NSOC seperti platform *threat intelligence,* sensor keamanan, dan dukungan perangkat lainnya yang digunakan oleh NSOC.

Siklus NSOC-VM juga diharapkan dapat menyesuaikan dengan perubahan dan dinamika yang terjadi. Peningkatan teknologi, beragamnya kerentanan dan ancaman, serta kebutuhan organisasi membuat NSOC harus dapat beradaptasi dan melakukan peningkatan. Apabila diperlukan, tim pendukung seperti Tim Forensik Digital, Analisis *Malware,* dan Infrastruktur dapat berperan aktif dalam siklus NSOC-VM. Tim Forensik Digital dan Tim Analisis *Malware* dapat berperan untuk analisis mendalam terkait kerentanan dan ancaman yang ditemukan. Tim Infrastruktur dapat berperan untuk pengelolaan sarana dan prasarana NSOC dalam pelaksanaan manajemen kerentanan, termasuk pengelolaan *platform* NSOC-VM apabila diterapkan pada NSOC. Adaptasi tersebut juga dapat dilakukan berdasarkan perkembangan regulasi dan peraturan baru seperti adanya usulan pembentukan *Special SOC* pada Ibu Kota Nusantara (IKN). Usulan ini dijelaskan dalam Peraturan Presiden Republik Indonesia No. 62 tahun 2022 tentang Perincian Rencana Induk Ibu Kota Nusantara (Presiden Republik Indonesia, 2022b). Dengan adanya ibu kota baru dan SOC khusus di dalamnya, maka harus dilakukan penyesuaian terhadap NSOC yang ada. Penyesuaian tersebut memerlukan penelitian dan analisis mendalam agar dapat tercipta kolaborasi antar SOC. Kolaborasi ini penting untuk diupayakan agar tugas dan fungsi SOC dapat dilaksanakan secara efektif dan optimal untuk memberikan dukungan pengamanan dan pelindungan IIV di Indonesia.

5. KESIMPULAN

Penelitian ini membahas terkait usulan kerangka kerja manajemen kerentanan pada NSOC untuk memberikan pelindungan pada IIV. Kontribusi yang diberikan melalui penelitian ini memiliki sintesis sebagai berikut,

a) Manajemen kerentanan sangat penting untuk diterapkan pada NSOC karena maraknya kerentanan dan ancaman siber yang menyasar pada IIV, kurangnya perbaikan dan remediasi yang dilakukan, dan belum adanya kerangka kerja yang dapat diterapkan. Diusulkan kerangka kerja NSOC-VM sebagai kerangka kerja manajemen kerentanan yang dapat diterapkan oleh NSOC sebagai SOC lingkup nasional untuk memberikan pelindungan pada IIV.
b) NSOC-VM disusun berdasarkan beberapa standar terkait keamanan informasi, pelindungan IIV, praktik terbaik pelaksanaan SOC, dan pelaksanaan manajemen kerentanan.
c) NSOC-VM terdiri dari empat tahapan, sepuluh aktivitas, dan tiga puluh lima rekomendasi penerapan. Hasil validasi oleh 10 pakar NSOC dengan wawancara terstruktur memperoleh hasil bahwa keseluruhan pakar setuju terhadap rancangan siklus NSOC-VM.
d) Penelitian ini dapat dilakukan pengembangan lebih lanjut berupa analisis penerapan kerangka kerja, pengembangan platform khusus, atau

penelitian mendalam terkait penyesuaian dengan standar, praktik terbaik, dan regulasi lain.

DAFTAR PUSTAKA

AFERUDIN, F., & RAMLI, K. 2022. The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia. *Budapest International Research and Critics Institute (BIRCI-Journal)*. https://doi.org/10.33258/birci.v5i3.6297

AVADANEI, A., NITESCU, L., CONSTANTIN, I., & SULTANOIU, C. P. 2021. Predictive Model for Software Vulnerability Management in Telecommunication Infrastructures. *2021 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2021*. https://doi.org/10.1109/BlackSeaCom52164.2021.9527768

BECKER, G., EISENBARTH, T., FEDERRATH, H., FISCHER, M., LOOSE, N., OTT, S., PECHOLT, J., MARWEDEL, S., MEYER, D., STIJOHANN, J., TALPUR, A., & VALLENTIN, M. 2024. SOVEREIGN - Towards a Holistic Approach to Critical Infrastructure Protection. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3664476.3671410

BECKVARD, H. P. 2022. Protecting Critical Infrastructure and Critical Information Infrastructure. *CONTEMPORARY MILITARY CHALLENGES*, *24*(2), 15–28. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.1

BSSN. 2022. *Keputusan Kepala Badan Siber dan Sandi Negara No. 248 tahun 2022 tentang Peta Proses Bisnis Badan Siber dan Sandi Negara*.

BSSN. 2023. *Lanskap Keamanan Siber Indonesia 2023*. https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

CHHILLAR, K., & SHRIVASTAVA, S. 2021. Vulnerability Scanning and Management of University Computer Network. *IEMECON 2021 - 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks*. https://doi.org/10.1109/IEMECON53809.2021.9689207

CISA. 2016. *CRR Supplemental Resource Guide Vulnerability Management Version 1.1*.

CISA. 2020. *Insider Threat Mitigation Guide*.

DAROJAT, E. Z., SEDIYONO, E., & SEMBIRING, I. 2022. Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner. *JURNAL SISTEM INFORMASI BISNIS*, *12*(1), 36–44. https://doi.org/10.21456/vol12iss1pp36-44

ENISA. 2020. *ISAC in a Box*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/view

FARRIS, K. A., SHAH, A., CYBENKO, G., GANESAN, R., & JAJODIA, S. 2018. VULCON: A system for vulnerability prioritization, mitigation, and management. *ACM Transactions on Privacy and Security*, *21*(4). https://doi.org/10.1145/3196884

FIRST. 2022. *TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0*. https://www.first.org/tlp/

HAN, C. H., PARK, S. T., & LEE, S. J. 2019. The Enhanced Security Control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. *International Journal of Critical Infrastructure Protection*, *26*. https://doi.org/10.1016/j.ijcip.2019.100312

HOMELAND SECURITY. 2013. *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*.

HORE, S., SHAH, A., & BASTIAN, N. D. 2023. Deep VULMAN: A deep reinforcement learning-enabled cyber vulnerability management framework. *Expert Systems with Applications*, *221*. https://doi.org/10.1016/j.eswa.2023.119734

ISO. 2018. *ISO/IEC 29147:2018 (Information technology — Security techniques — Vulnerability disclosure)*.

ISO. 2022. *Information security, cybersecurity and privacy protection-Information security controls*.

JOHNSON, C. S., BADGER, M. L., WALTERMIRE, D. A., SNYDER, J., & SKORUPKA, C. 2016. *Guide to Cyber Threat Information Sharing*. https://doi.org/10.6028/NIST.SP.800-150

KNERLER, K., PARKER, I., & ZIMMERMAN, C. 2022. *11 Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation.

LI, W., TIAN, K., & WANG, W. 2023. Research and Practice on Network Security Vulnerability Management Methods in the Transportation Industry. *ACM International Conference Proceeding Series*, 318–322. https://doi.org/10.1145/3661638.3661699

MAGNUSSEN, G. M. K., PETTERSEN, M., & NIEMIMAA, M. I. 2023. *A Comprehensive Framework for Patching and Vulnerability Management in Enterprises An Exploratory Study of How Enterprises Facilitate Patching and Vulnerability Management*. University of Agder.

MEHRI, V. A., ARLOS, P., & CASALICCHIO, E. 2022. Automated Context-Aware Vulnerability

Risk Management for Patch Prioritization. *Electronics (Switzerland)*, *11*(21). https://doi.org/10.3390/electronics11213580

MUTEMWA, M., MTSWENI, J., & ZIMBA, L. 2018. Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies and Information Technology Systems. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, 1–6. https://doi.org/10.1109/ICONIC.2018.8601251

NIKOLAOU, N., PAPADAKIS, A., PSYCHOGYIOS, K., & ZAHARIADIS, T. 2023. Vulnerability Identification and Assessment for Critical Infrastructures in the Energy Sector. *Electronics (Switzerland)*, *12*(14). https://doi.org/10.3390/electronics12143185

NIST. 2012. *NIST SP 800-30 Revision 1 - Guide for Conducting Risk Assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

NIST. 2020. *Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

NIST. 2024. *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

PALMAERS, T. 2021. *Implementing a Vulnerability Management Process Implementing a vulnerability management process 2*.

PRESIDEN REPUBLIK INDONESIA. 2022. *Peraturan Presiden No. 82 tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital*.

PRESIDEN REPUBLIK INDONESIA. 2022. *Peraturan Presiden Republik Indonesia No. 63 tahun 2022 tentang Rancangan Induk Ibu Kota Negara*.

PUSAT OPERASI KEAMANAN SIBER NASIONAL. 2021. *Grand Desain NSOC - National Security Operation Center*. BSSN.

PUTRO, P. A. W., & SENSUSE, D. I. 2021. Threats, Vulnerabilities and Security Functions in Critical Information Infrastructure. *2021 8th International Conference on Information Technology, Computer and Electrical Engineering, ICITACEE 2021*, 113–117. https://doi.org/10.1109/ICITACEE53184.2021.9617515

RECORDED FUTURE. 2022. *The Intelligence Handbook - A Roadmap for Building and Intelligence-Led Security Program* (4 ed.). CyberEdge Group, LLC.

ROSHANAEI, M. 2021. Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications*, *09*(08), 80–102. https://doi.org/10.4236/jcc.2021.98006

RUSSO, P., CAPONI, A., LEUTI, M., & BIANCHI, G. 2019. A web platform for integrated .