Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 5, No. 9, September 2025, Hal. 2605-2620
DOI: https://doi.org/10.52436/1.jpti.1015
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Peningkatan Kapabilitas *National Security Operations Center (NSOC)* Berbasis *Benchmarking* untuk Keamanan Siber Nasional

Nur Annisa Kadarwati Febriyani[*1], Muhammad Salman[2], Muhammad Azza Ulin Nuha[3]

[1,2,3]Teknik Elektro, Universitas Indonesia, Indonesia
Email: [1]nur.annisa22@ui.ac.id, [2]muhammad.salman@ui.ac.id, [3]muhammad.azza21@ui.ac.id

Abstrak

Peningkatan jumlah pengguna internet di Indonesia selama empat tahun terakhir turut meningkatkan jumlah anomali trafik siber, rata-rata mencapai 768 juta per tahun. Pemerintah Indonesia melalui Badan Siber dan Sandi Negara (BSSN) telah membentuk *National Security Operations Center* (NSOC) sebagai strategi keamanan siber nasional. Namun, implementasi NSOC menghadapi tantangan dalam hal kapabilitas, koordinasi, dan peningkatan operasional. Penelitian ini menggunakan metode studi literatur dan *benchmarking* terhadap praktik SOC dari Uni Eropa, Inggris, Amerika Serikat, dan Australia. Hasil kajian menunjukkan bahwa praktik terbaik SOC memiliki tujuh kapabilitas dan 42 aktivitas. Sementara itu, NSOC memiliki sembilan kapabilitas dengan sembilan aktivitas belum diimplementasikan. Rekomendasi yang disusun antara lain penambahan kapabilitas *Leadership and Management* dan penguatan aktivitas seperti penyusunan pedoman simulasi ancaman, penanganan ancaman internal, layanan manajemen kerentanan, otomatisasi *ticketing* respons insiden, serta mekanisme transfer pengetahuan antar personel. Penelitian ini memberikan kontribusi keilmuan berupa model peningkatan SOC berbasis *benchmarking* internasional dan dapat dijadikan acuan dalam kebijakan keamanan siber nasional.

Kata kunci: *Benchmarking, MITRE SOC Framework, NSOC, SOC.*

Enhancing the Capabilities of the National Security Operations Center (NSOC) Through Benchmarking for National Cybersecurity

Abstract

The significant increase in internet users in Indonesia over the past four years has led to a rise in cyber traffic anomalies, averaging 768 million incidents annually. In response, the Government of Indonesia, through the National Cyber and Crypto Agency (BSSN), has established the National Security Operations Center (NSOC) as part of its national cybersecurity strategy. However, the implementation of NSOC faces several challenges related to capability development, inter-agency coordination, and operational enhancement. This study employs a literature review and benchmarking methodology, comparing SOC practices in the European Union, the United Kingdom, the United States, and Australia. The findings indicate that the best practice SOCs exhibit seven capabilities and 42 associated activities, whereas the NSOC possesses nine capabilities with nine key activities yet to be implemented. Recommended improvements include the addition of Leadership and Management capability and the enhancement of activities such as threat simulation guideline development, internal threat handling, vulnerability management services, automated incident response ticketing, and knowledge transfer mechanisms. This research contributes to the body of knowledge by proposing a SOC capability enhancement model based on international benchmarking and offers a strategic reference for national cybersecurity policy formulation.

Keywords: *Benchmarking, MITRE SOC Framework, NSOC, SOC.*

1. PENDAHULUAN

Selama lebih dari dua dekade, internet memainkan peran yang signifikan dalam komunikasi global dan mengalami peningkatan integrasi ke dalam berbagai aspek kehidupan di seluruh dunia [1]. Di Indonesia, pertumbuhan pengguna internet mencapai 5,8% dalam empat tahun terakhir, dengan total pengguna sebanyak 221,56 juta jiwa atau 79,5% dari total populasi [2], [3]. Peningkatan pengguna internet dan aktivitas digital menyebabkan peningkatan ancaman siber secara signifikan [4]. BSSN mencatat rata-rata 768 juta anomali trafik per tahun dalam lima tahun terakhir [5], [6], [7], [8], [9]. Jumlah tersebut tiga kali lebih tinggi dari jumlah pengguna

p-ISSN: 2775-4227
e-ISSN: 2775-4219

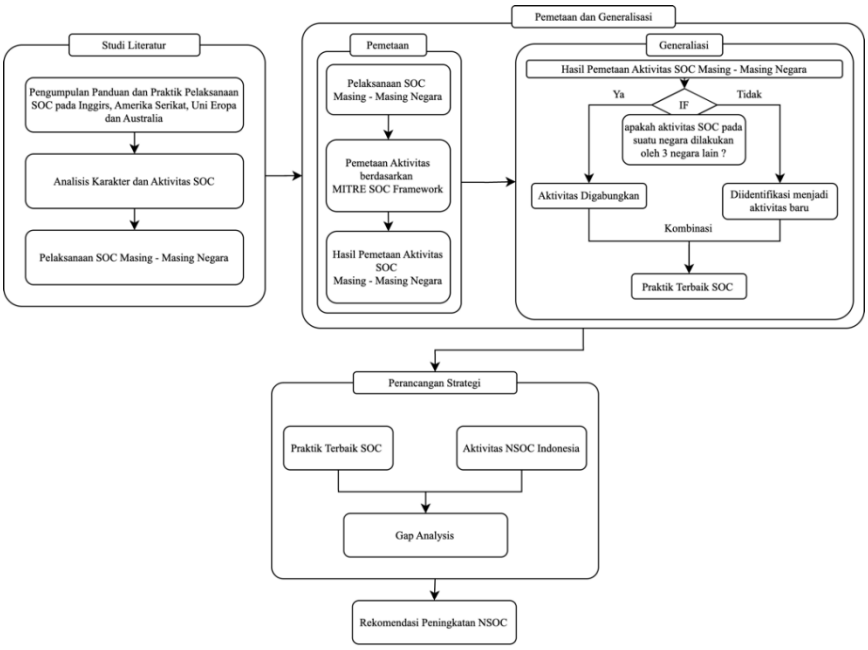
internet. Informasi ini menunjukkan bahwa isu keamanan siber memerlukan perhatian khusus dan strategi yang adaptif serta berkelanjutan.

Pemerintah Indonesia telah membentuk BSSN sebagai lembaga yang memiliki tanggung jawab dalam penanganan keamanan siber melalui Peraturan Presiden Nomor 28 Tahun 2021 [10]. Penerapan strategis dilakukan oleh BSSN dengan membentuk *Security Operation Center* (SOC) atau Pusat Operasi Keamanan Siber Nasional yang berfungsi sebagai *National* SOC dan berperan sebagai pusat koordinasi nasional dalam deteksi dan respons insiden siber (NSOC) [11] dan selanjutnya, seiring dengan restrukturisasi organisasi, pengelolaannya berada di bawah Direktorat Operasi Keamanan Siber [12]. Namun, pelaksanaan NSOC masih menghadapi berbagai kendala antara lain koordinasi yang belum optimal dengan stakeholder, kesenjangan dalam respons terhadap notifikasi insiden [9] serta keterbatasan sistem monitoring terhadap seluruh titik kritis di Indonesia [13].

Untuk mengatasi tantangan tersebut, diperlukan strategi peningkatan kapabilits NSOC yang berorientasi pada praktik keamanan siber secara global. Berbagai negara telah melakukan upaya untuk mengatasi tantangan dalam penanganan insiden siber melalui penerbitan pedoman pembangunan SOC, seperti *Massachusetts Institute of Technology Research and Engineering* (MITRE) [14], *European Union Agency for Cybersecurity* (ENISA) [15], dan *Cybersecurity and Infrastructure Security Agency* (CISA) [16]. Studi literatur dan *benchmarking* terhadap pedoman-pedoman tersebut dapat dilakukan untuk merancang strategi peningkatan keamanan siber, khususnya pada aspek penguatas SOC. Pendekatan serupa telah digunakan oleh Dedeke dan Materson dengan membandingkan *framework* keamanan siber dari tiga negara untuk merumuskan usulan peningkatan berdasarkan praktik terbaik, dengan mempertimbangkan karakteristik pendekatan masing-masing negara [17]. Penelitian serupa dilakukan oleh Nuha dkk. yang membandingkan implementasi *framework* keamanan siber dari berbagai negara guna merumuskan *Vulnerability Management Cycle* yang sesuai bagi Indonesia [18].

Penelitian ini bertujuan melakukan pemetaan menyeluruh terhadap kapabilitas dan aktivitas NSOC berdasarkan *benchmarking* terhadap pelaksanaan SOC dari empat negara acuan versi *Global Cybersecurity Index* (GCI) tahun 2024. Penelitian ini juga memberikan keterbaruan penelitian berupa usulan rekomendasi berbasis analisis *gap* pada pelaksanaan NSOC di Indonesia. Tujuan utama penelitian ini adalah melakukan identifikasi praktik terbaik SOC secara global, membandingkannya dengan pelaksanaan NSOC di Indonesia, dan merumuskan rekomendasi strategis untuk peningkatan kapabilitas NSOC. Hasil penelitian ini diharapkan dapat berkontribusi pada penguatan kebijakan keamanan siber nasional yang lebih terstruktur, responsif terhadap insiden, dan adaptif terhadap kompleksitas ancaman siber di masa mendatang.

2. METODE PENELITIAN



Gambar 1. Alur Metodologi Penelitian

Penelitian ini menggunakan pendekatan metode penelitian berupa *benchmarking* untuk perancangan strategi yang berkaitan dengan keamanan siber yang telah digunakan pada penelitian Dekeke dan Matersons [17] dan Nuha et.al [18] pada penelitian sebelumnya yang kemudian disesuaikan dengan kebutuhan penelitian. *Benchmarking*

p-ISSN: 2775-4227
e-ISSN: 2775-4219

digunakan karena negara-negara dengan peringkat GCI yang tinggi memiliki standar keamanan siber yang baik termasuk dalam penyelenggaraan SOC. Selain hal tersebut, benchmarking dalam ranah perancangan strategi peningkatan SOC dipilih karena dapat membantu untuk mengidentifikasi praktik terbaik yang telah dilakukan oleh berbagai negara [17], menilai kekurangan dalam aktivitas penyelenggaraan NSOC saat ini [19] [20], dan membantu dalam menentukan strategi peningkatan yang perlu dilakukan [21] [22]. Atas dasar tersebut, tahapan penelitian yang dilakukan pada penelitian ini diantaranya studi literatur, pemetaan dan generalisasi aktivitas, dan perancangan strategi yang digambarkan pada Gambar 1.

2.1. Studi Literatur

Pada tahap studi literatur, dilakukan analisis mendalam terhadap panduan implementasi SOC yang diterbitkan dari berbagai negara. Pemilihan negara yang digunakan sebagai sampel menggunakan negara yang dicantumkan dalam penelitian Dekeke dan Mastersons [17] dan Ulin Nuha et.al [18] yakni Amerika Serikat, *United Kingdom* (UK), Uni Eropa, dan Australia. Selain digunakan pada penelitian sebelumnya, pemilihan negara yang digunakan pada penelitian ini mempertimbankan posisi negara tersebut pada *Global Cybersecurity Index* 2024 yang menempati Level T1 yakni *role modelling* [23], sehingga dapat menjadi acuan dalam penyelenggaraan SOC. Dalam tahap ini, akan dipelajari mengenai karakteristik atktivitas implementasi SOC masing – masing negara. Sehingga, setelah tahap ini usai aktivitas implementasi SOC masing – masing negara akan teridentifikasi.

2.2. Pemetaan dan Generalisasi Aktivitas

Hasil identifikasi aktivitas yang dilakukan oleh SOC masing-masing negara, selanjutnya dipetakan berdasarkan kapabilitas SOC menutur MITRE SOC *Framework*. Adapun kapabilitas SOC berdasarkan MITRE SOC *Framework* terdiri dari 7 kapabilitas diantaranya sebegai berikut:

a. *Incident Triage, Analysis, and Response*
b. *Cyber Threat Intelligence, Hunting, and Analytics;*
c. *Expanded SOC Operations; Vulnerability Management;*
d. *SOC Tools, Architecture, and Engineering;*
e. *Situational Awareness, Communication, and Training;*
f. *Leadership Management.*

Pemetaan aktivitas SOC yang dilakukan dari masing-masing negara bertujuan untuk mendapatkan figur yang lengkap dari aktivitas SOC yang didefinisikan oleh masing-masing negara sesuai dengan kapabilitas yang seharusnya dimiliki oleh sebuah SOC dan diperoleh persamaan maupun perbedaan aktivitas antara negara. Kekurangan aktivitas yang ada di suatu negara dapat dilengkapi dengan aktivitas negara lain. Setelah dilakukan pemetaan, seluruh aktivitas yang terdefinisi akan dilakukan generalisasi untuk mendapatkan praktik terbaik aktivitas SOC yang dikumpulkan dari berbagai negara berdasarkan kapabilitas yang harus dimiliki oleh SOC.

2.3. Perancangan Strategi

Hasil generalisasi kapabilitas dan aktivitas praktik SOC yang diperoleh dari berbagai negara selanjutnya dibandingkan dengan kondisi kapabilitas dan aktivitas yang dijalankan oleh NSOC saat ini. Hasil perbandingan menghasilkan informasi kapabilitas maupun aktivitas mana saja yang belum diakomodir oleh NSOC dan menjadi rekomendasi strategi peningkatan NSOC di masa yang akan datang.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Implementasi SOC Global

Pada bagian ini akan dibahas mengenai hasil analisis terhadap standar, peraturan, maupun publikasi terkait implementasi SOC pada 4 (empat) negara berikut.

3.1.1. Implementasi SOC pada Uni Eropa

Uni Eropa memiliki ENISA, yang merupakan *Union's Agency* yang menjalankan tugasnya dalam bidang keamanan siber di Kawasan Uni Eropa. Berkaitan dengan pelaksanaan SOC, di Tahun 2020 ENISA menerbitkan *guideline* yang bertajuk *"How To Setup CSIRT and SOC"* sebagai panduan dalam menyelenggarakan SOC. Dalam dokumen ini tahapan dalam mendirikan atau melakukan pengaturan SOC terdiri dari 6 siklus pembentukan, yaitu *Assessment for Readiness, Design, Implementation, Operations,* dan *Improvement*. Berdasarkan alur tersebut aktivitas yang perlu dilakukan dalam pembangunan sebuah SOC diantaranya sebagai berikut[15].

p-ISSN: 2775-4227
e-ISSN: 2775-4219

a. Penilaian kesiapan organisasi dalam menjalankan SOC. Dalam aktivitas ini juga dilakukan diskusi untuk menentukan tujuan dari penyelenggaraan SOC, dan penentuan anggaran dan kebutuhan yang diperlukan untuk pembentukan desain dari SOC.
b. Pembentukan desain atau perencanaan dari penyelenggaraan SOC. Berdasarkan aktivitas ini, perencanaan yang dibutuhkan ialah bagaimana struktur organisasi dari SOC yang dibangun; ;kebutuhan personel dari segi kapabilitas dan tanggung jawab, rencana pelaksanaan layanan SOC seperti *Information Security Incident Management, Vulnerability Management, Situational Awareness, Knowledge Transfer,* dan *Information Security Event Management*; teknologi yang digunakan dalam pelaksanaan SOC dan bagaimana pengelolaannya; dan rencana kerjasama SOC dengan mitra negara lain.
c. Penjalanan layanan yang sudah direncanakan sebelumnya. Pada aktivitas ini layanan *Information Security Incident Management, Vulnerability Management, Situational Awareness, Knowledge Transfer,* dan *Information Security Event Management* diselenggarakan secara terus menerus secara bertahap sembari organisasi melakukan pemenuhan fasilitas, perangkat, maupun personel hingga rencana yang telah didefinisikan sebelumnya terwujud sepenuhnya.
d. Pengukuran aktivitas mapun layanan yang telah diselenggarakan sebelumnya. Pengukuran dilakukan baik secara internal maupun eksternal organisasi SOC. Pengukuran internal dilakukan terhadap pemenuhan *Key Performance Indicator* (KPI) SOC secara berkala untuk menilai efektivitas, ketermanfaatan, dan relevansi layanan yang diselenggarakan oleh SOC. Penilaian secara eksternal dilakukan oleh stakeholder SOC, diantaranya adalah penerima layanan dan mitra untuk mendapatkan masukan tambahan terkait penyelenggaraan SOC yang telah dilakukan.
e. Penyusunan langkah peningkatan perubahan berdasarkan hasil evalulasi layanan maupun aktivitas yang diselenggarakan oleh SOC yang diperoleh baik dari internal SOC maupun eksternal SOC.

3.1.2. Implementasi SOC di Australia

Australia memiliki lembaga pemerintah yang secara aktif bertanggung jawab dalam mengoordinasikan upaya keamanan siber nasional serta menyusun pedoman-pedoman terkait keamanan siber, yaitu *Australian Cyber Security Centre* (ACSC). ACSC memiliki berbagai peran meliputi pusat kontak insiden siber nasional, pemberian panduan teknis keamanan siber, pemantauan ancaman siber, berbagi informasi keamanan siber antar organisasi, dan pelatihan untuk peningkatan keamanan siber di Australia. Peran-peran tersebut dilakukan bersama dengan *Minister of Defence* Australia.

ACSC mengeluarkan berbagai panduan mengenai tata kelola keamanan siber yang dapat diacu oleh organisasi swasta maupun pemerintahan. Praktik tata kelola keamanan siber di lingkup pimpinan organisasi dijelaskan melalui *"Practical Cybersecurity Tips for Business Leaders"*. Pimpinan organisasi diberikan panduan untuk pengamanan terhadap perangkat, akun, sosial media, komunikasi, dan mobilitas [24]. Publikasi lengkap mengenai penerapan keamanan siber teknologi informasi dan operasional organisasi melalui *Information Security Manual*. Publikasi ini memuat berbagai macam kontrol yang dapat diterapkan oleh organisasi dalam melakukan pengamanan informasi [25]. Pendekatan berbasis risiko digunakan oleh organisasi untuk melakukan berbagai aktivitas, seperti identifikasi aset, respon ancaman, dan pengamanannya. ACSC juga memberikan kebijakan manajemen risiko bagi keamanan *supply chain* atau rantai pasok. Pemanfaatan *articial intelligence* (AI) diatur melalui tata kelola pemanfaatan *artificial intelligence*. Di dalamnya mengatur penerapan AI meliputi prinsip *secure by design,* keamanan dan privasi data, dan manajemen penggunaannya.

Pelaksanaan identifikasi dilakukan dengan berbagai kegiatan seperti manajemen aset teknologi informasi dan teknologi operasional, khususnya pada lungkup infrastruktur informasi vital. Identifikasi terhadap berbagai ancaman siber dilakukan terhadap berbagai hal seperti *data breach, cryptomining, hacking, malware, phising, ransomware,* dan *scam*. ACSC juga memberikan informasi mengenai langkah-langkah untuk meningkatan kematangan siber melalui *maturity level* dengan skala 0 hingga 3 sebagai sarana peningkatan organisasi [26].

Pada pelaksanaan proteksi, ACSC menerbitkan kebijakan mengenai kontrol keamanan informasi dalam dokumen *Information Security Manual*. Penerapan autentikasi multifaktor dijelaskan melalui panduan *Multi-factor Authentication*. Peningkatan kesadaran keamanan siber disebarluaskan melalui berbagai publikasi seperti penanganan *social engineering,* serangan melalui email dan sosial media, dan tips keamanan siber saat bepergian. Panduan pengamanan spesifik dijelaskan untuk pengamaman pada perangkat elektronik, akun akses, dan email.

ACSC melaksanakan deteksi dengan melakukan monitoring insiden siber setiap hari dalam satu minggu. Dalam lingkup *threat intelligence,* ACSC memiliki program *Cyberthreat Intelligence Sharing* (CTIS) sebagai sarana berbagi informasi ancaman siber antara pemerintah dan industri. Hasil analisis APT dan ancaman siber dipublikasikan melalui *Cyber Threat Report* [27]. Terdapat panduan mengenai monitoring sistem secara terpusat, mendeteksi aktivitas yang berbahaya, penyimpanan log, memberlakukan retensi log dengan benar. Penanganan

p-ISSN: 2775-4227
e-ISSN: 2775-4219

terhadap *insider threat* dipublikasikan melalui panduan penanganan *insider threat* meliputi penerapan kontrol dan audit.

Pelaksanaan respon insiden siber dilakukan ACSC dengan menerima pelaporan insiden. Pelaporan insiden tersebut diterima melalui *hotline* khusus. Insiden tersebut mendapatkan asistensi hingga forensik digital. Panduan-panduan penanganan berbagai insiden siber yang dikeluarkan dapat dijadikan sebagai rujukan bagi organisasi-organisasi lain dalam melakukan praktik manajemen insiden. ACSC juga menyusun panduan pemulihan insiden siber untuk berbagai insiden yang bersifat kritikal seperti *data breach, account compromise, malware,* dan *ransomware* untuk standardisasi pelayanan pasca insiden.

3.1.3. Implementasi SOC di Inggris

Inggris memiliki sebuah lembaga yang bertanggung jawab atas keamanan siber bagi organisasi kritikal, sektor publik, industri, swasta, dan pemerintahan yang dimakan *National Cyber Security Centre* (NCSC). Secara umum, tugas yang dilenggarakan oleh NCSC ialah penyusunan panduan keamanan siber, melakukan insiden respons atas insiden keamanan siber yang terjadi di Inggris, meningkatkan kapabilitas keamanan siber UK dengan memanfaatkan ahli dibidang insdustri dan akademik di Inggris, dan menurunkan risiko ancaman siber di Inggris dengan melakukan pengamanan jaringan pada sektor publik dan privat. Berkaitan dengan penyelenggaraan SOC, terdapat beberapa panduan yang telah disusun. Panduan yang pertama dikeluarkan pada Tahun 2022, terkait aspek yang perlu diperhatikan dalam pembangunan SOC [28].

a. Penyusunan/penentuan *Operating Model* yang digunakan sebagai dasar bagi organisasi untuk mereplikasi dan memahami komponen yang dibutuhkan dalam membangun SOC. Penyusunan *operating model* SOC harus didasari atas *threat profile* organisasi dan aset yang dilindungi oleh organisasi.
b. *Onboarding* atau Proses penambahan sistem ke dalam cakupan SOC. Dalam proses *onboarding*, *log* dari sistem tersebut dipastikan dapat terkumpul atau terkirim ke sistem SOC, sehingga dapat dipantau. Untuk mempermudah proses *onboarding* dapat menggunakan pendekatan *threat modelling* untuk menentukan *log* apa saja yang berguna dalam proses deteksi serangan siber
c. Deteksi atau ruang lingkup deteksi yang membahas pendekatan yang dapat dilakukan untuk mendeteksi serangan siber. Dalam pendeteksian serangan siber, pemilihan *tools* dapat disesuaikan dengan intensitas serangan siber dan attack sophistication. Opsi yang dapat dipilih seperti aplikasi berlisensi (Anti-*malware tools*, IDS), *custom detection use-case*, *data mining*, atau *threat hunting* selain pemilihan alat, pertimbangan lain yang perlu diperhatikan dalam deteksi ialah pemahaman mengenai kondisi normal organisasi, kebutuhan platform untuk analisis *log*, minimalisasi *false positive*, dan pengelolaan *use-case* deteksi.
d. *Threat intelligence* yang digunakan mendukung peningkatan kapasitas deteksi pada SOC jika pendekatan deteksi yang diadopsi tidak menggunakan aplikasi komersil. Hal ini dikarenakan dalam *threat intelligence* terdapat pengetahuan mengenai aktivitas yang dilakukan oleh penyerang, yang dapat mencakup mulai dari motivasi, hingga *tactic, techniques, and procedures* yang digunakan oleh *threat actor*. Pendekatan yang dapat digunakan untuk mengimplementasikan *threat intelligence* ialah implementasi penggunaan *Threat Intelligence Platform* dan Penyelenggaraan *Intelligence Sharing.*
e. *Incident Response dan Management* yang digunakan sebagai dasar bagi organisasi untuk merespons insiden yang terjadi pada organisasi dan mengelola insiden yang terjadi. Dalam aspek ini perlu memerhatikan dengan bagaimana proses triase yang dilakukan organisasi untuk membedakan antara insiden dan *alert*, dan perlunya *cybersecurity exercise* bagi organisasi untuk meningkatkan kemampuan personel SOC untuk menangani insiden maupun meningkatkan efisiensi penanganan insiden yang dilakukan oleh organisasi.

NCSC juga memberikan panduan – panduan lain yang dapat digunakan bagi personel SOC ketika menjalankan berbagai fungsi yang diselenggarakan oleh SOC. Terkait dengan fungsi deteksi, NCSC menerbitkan panduan mengenai bagaimana pengelolaan *log* maupun pemanfaatan log yang digunakan untuk mendukung pendeteksian serangan maupun respons insiden. Panduan ini bertajuk *"Introduction to logging for security purposes"*[29]. Panduan mengenai bagaimana proses *threat hunting* dapat diimplementasikan terhadap organisasi juga disediakan dalam tajuk *"Detection the Unknown: A Guide to Threat Hunting". Guideline* ini menjelaskan bagaimana *threat hunting* dapat diadopsi oleh organisasi dan membantu organisasi dalam meningkatkan kemampuan deteksi ancaman siber yang rumit atau baru[30].

Dukungan untuk fungsi *Threat Intelligence* juga disediakan oleh NCSC. Yang pertama melalui pemanfaatan *Threat Intelligence* bagi pimpinan maupun level teknis dalam tajuk *"Cyber Threat Intelligence in Government: A Guide for Desicion Makers & Analyst".* Panduan ini dapat membantu organisasi dalam proses investigasi insiden maupun mempersiapkan organisasi untuk menghadapi serangan siber yang sudah terlebih dahulu terjadi di negara lain[31]. Selain panduan tersebut, NCSC juga membentuk *Platform Cyber Security Information Sharing*

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Partnership (CISP) yang menjadi wadah bagi pegiat keamanan siber di Inggris untuk berbagi *threat information* [32].

Dukungan pelaksanan Incident Management disediakan bentuk penyediaan laman khusus pelaporan insiden [33] dan panduan mengenai bagaimana proses *incident management* dilakukan dalam tajuk "*Incident Management*: *How to effectively detect, respond to and resolve cyber incidents*". Panduan ini memberikan langkah – langkah maupun hal yang dapat menjadi pertimbangan dalam melakukan proses respons insiden dan manajemen insiden[34]. Selain panduan, NCSC juga menyediakan *resource* yang dapat digunakan organisasi untuk melakukan *cybersecurity exercise* dalam tajuk "*Exercise in a Box*" yang dapat digunakan SOC untuk melatih dan meningkatkan kemampuan SOC dalam merespon insiden[35].

3.1.4. Implementasi SOC di Amerika Serikat

Cybersecurity & Infrastructure Security Agency (CISA) merupakan organisasi yang bertanggung jawab terhadap pertahanan siber Amerika Serikat. Untuk memenuhi tanggung jawab tersebut, CISA memegang tugas sebagai koordinator keamanan dan ketahanan infrastruktur kritikal nasional di Amerika. Dalam rangka menjalankan tugasnya, CISA menjalankankan beberapa program dan menerbitkan berbagai panduan yang dapat digunakan bagi organisasi untuk mengimplementasikan SOC.

Pelaksanaan identifikasi dilakukan dengan berbagai kegiatan seperti manajemen risiko dan manajemen aset. Pelaksanaan manajemen risiko dilakukan melalui *National Risk Management Center*. Selain penjalanan program tersebut, CISA menerbitkan panduan mengenai pengelolaan yang dapat digunakan oleh organisasi untuk mengelola aset berdasar risiko aset. Panduan ini mengatur bagaimana organisasi mulai merencanakan pengelolaan aset, mengidentifikasi aset, hingga mengevaluasi inventarisasi aset yang telah dilakukan[36].

Pada pelaksanaan proteksi, CISA menerbitkan kebijakan/panduan mengenai bagaimana manajemen kontrol [37], manajemen kerentanan [38] , dan pembangunan kesadaran keamanan informasi [39] dapat diterapkan organisasi. Melalui *Joint Cyber Defence Collaborative,* CISA membangun kerjasama dalam melakukan proteksi terhadap ancaman siber. Dalam hal peningkatan kesadaran keamanan, CISA menyediakan layanan *capacity building* untuk meningkatkan *skill* dan kemampuan keamanan siber yang dapat diakses oleh seluruh kalangan melalui *website* CISA.

CISA melaksanakan deteksi dengan melakukan *threat hunting* berdasarkan aset yang dikelolanya. Dalam lingkup *threat intelligence,* CISA memiliki program *Cyberthreat Intelligence Sharing* (CTIS) sebagai sarana berbagi informasi ancaman siber antar pemerintahan. Informasi yang dibagikan meliputi *Indicators of Compromise* (IoC), *Application Programming Interfaces* (APIs), *threat platform tools*, dan pelatihan dalam *threat intelligence*[40].

Kegiatan respons insiden dilakukan oleh CISA melalui penerimaan pelaporan insiden. Pelaporan insiden tersebut diterima melalui *website* khusus dan organisasi dapat mengajukan asistensi dalam penanganan insiden tersebut. Selain penerimaan laporan CISA juga memandu organisasi yang mengalami insiden melalui beberapa panduan maupun *playbook* yang disediakan. Beberapa panduan diantaranya *Cyber Incident Resource Guide for Governor* yang dapat digunakan oleh sektor pemerintahan ketika mengalami insiden siber [41]. Selain sektor pemerintahan, panduan pengelolaan insiden bagi organisasi juga diterbitkan oleh CISA dengan bekerjasama dengan Carneige Mellon *University*. Panduan ini menjelaskan langkah – langkah yang dapat dilakukan oleh organiasi untuk mengelola insiden, dari mulai mendeteksi insiden, melakukan triase, merespons, dan melakukan pemulihan pasca insiden[42].

3.2. Generalisasi dan Komparasi Aktivitas Penyelenggaraan SOC

Hasil analisis terhadap standar, peraturan, maupun publikasi terkait implementasi SOC digunakan untuk melakukan identifikasi aktivitas yang dilakukan oleh SOC dari masing-masing negara. Untuk mendapatkan keseragaman dalam gambaran implementasi SOC, hasil analisis di dipetakan ke dalam kapabilitas SOC yang dipublikasikan oleh MITRE. Untuk mempermudah dalam proses generalisasi dan analisis perbandingan, hasil pemetaan aktivitas SOC dari berbagai disajikan pada Tabel 1 berikut.

Tabel 1. Hasil Pemetaan Aktivitas SOC dari Berbagai Negara ke MITRE SOC *Framework*

SOC Capability	Negara	Aktivitas
Incident Triage, Analysis, and Response	Uni Eropa	1. Penyelenggaraan Layanan *Information Security Incident Management.* 2. Penyelenggaraan Layanan *Information Security Event Management.*

p-ISSN: 2775-4227
e-ISSN: 2775-4219

SOC Capability	Negara	Aktivitas
	Inggris	1. Melakukan penyusunan panduan untuk melakukan triase *alert*, mencari sumber *log* yang diperiksa, sistem yang diselidiki, dan bagaimana cara mengkomunikasikan alert yang terjadi. 2. Melakukan penyusunan dokumen perencanaan insiden respon yang memuat kontak yang dapat dihubungi, bagaimana alur proses insiden respon. 3. Melakukan penyusunan *playbook* untuk tipe insiden tertentu. 4. Malekukan penyusunan panduan tindakan kepatuhan atas regulasi pada saat terjadi insiden siber. 5. Memastikan informasi yang penting dalam proses respons insiden tersedia dengan baik. 6. Melakukan pengelolaan *log* yang digunakan sebagai *evidence* dalam proses respons insiden. 7. Melakukan triase insiden. 8. Melakukan mitigasi kepada aset, agar insiden tidak berdampak pada aset lain. 9. Melakukan investigasi dan analisis insiden siber. 10. Melakukan perbaikan terhadap aset terdampak insiden siber. 11. Memastikan hasil perbaikan berjalan dengan baik dan proses bisnis berjalan seperti semula.
	Amerika Serikat	1. Menyediakan *platform* khusus untuk pelaporan insiden. 2. Menyediakan layanan asistensi penanganan insiden. 3. Menyediakan panduan pengelolaan insiden.
	Australia	1. Menyediakan hotline secara nasional sebagai sarana penerimaan laporan insiden siber. 2. Memberikan pelayanan asistensi insiden hingga dukungan forensik digital. 3. Mempublikasikan panduan penanganan berbagai macam ancaman dan insiden siber. 4. Melakukan monitoring ancaman siber dan kontak siber selama 24/7.
CTI, Hunting, and Analytics	Uni Eropa	1. Menyediakan informasi ancaman siber terkini berdasarkan isu keamanan siber yang sedang menjadi perhatian.
	Inggris	1. Implementasi penggunaan threat intelligence platform sebagai sumber informasi. 2. Menyelenggarakan intelligence sharing untuk bertukar informasi ancaman siber. 3. Melakukan impelemntasi threat hunting untuk mengidentifikasi ancaman berupa unknown attack. 4. Melakukan pengembangan tools deteksi yang berbasis use-case dengan memanfaatkan serangkaian alert rules untuk mendeteksi serangan siber.
	Amerika Serikat	1. Menyelenggarakan Program *Cyber Threat Intelligence Sharing* antara instansi pemerintah. 2. Menyediakan layanan *Threat Hunting.*
	Australia	1. Menyelenggarakan program Cyber Threat Intelligence Sharing antara instansi pemerintah dan swasta. 2. Melakukan koordinasi untuk pemantauan ancaman siber terhadap mitra CERT negara lain.
Expanded SOC Operations	Uni Eropa	1. Melakukan publikasi mengenai panduan untuk melakukan simulasi ancaman siber. 2. Mempublikasikan panduan untuk penanganan *insider threat.*
	Inggris	1. Melakukan reviu dan pengujian kapabilitas teknologi yang digunakan dalam penanganan insiden.
	Amerika Serikat	1. Mempublikasikan panduan mitigasi *insider threat.*

p-ISSN: 2775-4227
e-ISSN: 2775-4219

SOC Capability	Negara	Aktivitas
	Australia	1. Merilis panduan mengenai penanganan *insider threat.* 2. Melakukan publikasi panduan dan pelatihan terhadap respons ancaman siber.
Vulnerability Management	Uni Eropa	1. Penyelenggaraan Layanan *Vulnerability Management.*
	Inggris	3. Melakukan pemetaan aktivitas aset, peran dari aset, *data flow*, dan *user behaviour* atas aset dan tingkat keamanan aset. 4. Menentukan skala prioritas dari aset dan dampak ketika terjadi kegagalan dalam berjalannya aset.
	Amerika Serikat	1. Penyelenggaraan Layanan *Vulnerability Management.* 2. Melakukan publikasi mengenai panduan penyelenggaraan *vulnerability management.*
	Australia	1. Mempublikasikan panduan pelaksanaan penilaian kerentanan. 2. Melakukan publikasi mengenai pengelolaan *patching* aplikasi dan sistem operasi secara berkala.
SOC Tools, Architecture, and Engineering	Uni Eropa	1. Melakukan pencadangan server untuk memastikan *availability* dan kebutuhan *recovery* pada *tools* SOC. 2. Melakukan pengaturan segmentasi jaringan pada SOC. 3. Mempertimbangkan penggunaan *tools* otomatisasi dalam *ticketing* penanganan insiden. 4. Mempertimbangkan penggunaan *tools* otomatisasi untuk *routing data threat intelligence.* 5. Mempertimbangkan penggunaan *tools* otomatisasi untuk penerbitan *alert* dan buletin dalam rangka mendukung *security awareness.*
	Inggris	1. Pengembangan *use-case* deteksi yang digunakan pada SIEM berdasarkan data anomali trafik yang dimiliki oleh SOC.
	Amerika Serikat	1. Penyelenggaraan layanan kerjasama pengembangan pengamanan terhadap ancaman siber.
	Australia	1. Menerbitkan panduan dalam pelaksanaan deteksi anomali dan penanganan *log.* 2. Mempublikasikan panduan desain jaringan dan infrastruktur TI yang aman.
Situational Awareness, Communications, and Training	Uni Eropa	1. Pelaksanaan Layanan *Situational Awareness.* 2. Pelaksanaan mekanisme *Knowledge Transfer* yang dilakukan antar personel SOC. *3.* Penyusunan *alert* dan buletin untuk meningkatkan *security awareness.* 4. Pelaksanaan pelatihan bagi personel SOC yang sesuai dengan kapabilitas SOC dan spesialiasi personel. 5. Membangun komunikasi dan kerjasama dengan konstituen, partner, dan stakeholder SOC. 6. Melakukan diseminasi layanan SOC kepada media, stakeholder, dan konstituen SOC.
	Inggris	1. Melakukan pembangunan CSIRT yang bertugas dalam menangani atau mesepons insiden. 2. Melakukan berbagai kegiatan untuk membangun kesadaran keamanan informasi maupun penanganan respons insiden dilevel Pimpinan. 3. Meningkatkan *security awareness* melalui pemberian berita keamanan siber bagi pegawai maupun pimpinan. 4. Melakukan *cybersecurity exercise* berdasarkan dengan menggunakan skenario insiden yang sebenarnya. 5. Memberikan pelatihan yang spesifik bagi staf maupun analis insiden. 6. Melakukan *cybersecurity exercise* secara berkala.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

SOC Capability	Negara	Aktivitas
		7. Melakukan pelatihan dan perancangan peta karir untuk personel SOC.
	Amerika Serikat	1. Menyediakan pelatihan keamanan siber yang terbuka secara umum di dalam *platfrom* CISA. 2. Menerbitkan informasi ancaman siber sesuai dengan isu terkini.
	Australia	1. Melakukan edukasi dan pelatihan kesadaran keamanan informasi secara umum. 2. Menerbitkan panduan dalam komunikasi ketika insiden dan pemulihan insiden siber. 3. Melakukan distribusi informasi ancaman siber secara berkala kepada sektor-sektor kritikal.
Leadership and Management	Uni Eropa	1. Melakukan penilaian kesiapan dari SOC dengan mempertimbangkan latar belakang SOC, struktur dari SOC, organisasi penyelenggara SOC, dan anggaran yang dimiliki oleh SOC. 2. Melakukan perencanaan penyelenggaraan SOC yang mencakup latar belakang SOC, rencana layanan/kapabilitas yang disediakan oleh SOC, rencana alur kerja, rencana skillset personel SOC, rencana pelatihan personel SOC, rencana fasilitas SOC, rencana penggunaan teknologi pada SOC, rencana kerjasama SOC, rencana manajemen keamanan teknologi informasi pada SOC. 3. Mengukur *Key Performance Indicator* dari penyelenggaraan SOC yang dilakukan. 4. Melakukan reviu performa layanan SOC secara tahunan yang dinilai dari kemampuan staf, proses bisnis, *tools* SOC, dan analisis KPI SOC. 5. Melakukan pertemuan tahunan dengan *stakeholder* SOC untuk mendapatkan reviu atau masukan untuk peningkatan SOC. 6. Melakukan perencanaan *budget* SOC berdasarkan rencana peningkatan SOC. 7. Melakukan penyusunan rencana peningkatan SOC yang didasarkan hasil reviu penyelenggaraan SOC.
	Inggris	1. Melakukan penyusunan operating model SOC atau dokumen perencanaan yang memuat komponen yang ada pada SOC (CTI, peningkatan kapabilitas, deteksi dan respons, tim pendukung), layanan yang dijalankan SOC (*Threat Intelligence, Threat Hunting, Content Development, Engineering, Incident Handling, Incident Management, Vulnerability Management, Insider Threat*), bagaimana dukungan operasi dari SOC, bagaimana kebutuhan resources dari SOC (*skill set*, analis SOC, dan perputaran analis), Tata Kelola SOC, bagaimana proses penyusunan rencana peningkaan dan keberlanjutan SOC, dan bagaimana cara untuk menjaga keamanan SOC. 2. Melakukan reviu terhadap prosedur dan panduan yang telah disusun. 3. Melakukan reviu pasca insiden.
	Amerika Serikat	1. Menerbitkan panduan penanganan insiden bagi pimpinan pemerintahan. 2. Menerbitkan panduan pengelolaan insiden.
	Australia	1. Menerbitkan panduan kebijakan keamanan siber bagi pimpinan organisasi.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

SOC Capability	Negara	Aktivitas
		2. Mempublikasikan tata kelola risiko dan manajemen terhadap rantai pasok. 3. Menyediakan publikasi mengenai pengelolaan risiko keamanan siber di lingkup organisasi.

Hasil pemetaan aktivitas pada Tabel 1, selanjutnya dilakukan proses generalisasi untuk mendapatkan gambaran mengenai aktivitas SOC terbaik dari berbagai negara. Proses generalisasi aktivitas SOC yang telah dipetakan pada tahap sebelumnya dilakukan menggabungkan aktivitas SOC yang dari beberapa negara yang dinilai memiliki jenis yang sama dan menambahkan aktivitas baru ketika aktivitas yang didefinisikan pada suatu negara tidak diselenggarakan di negara lain. Berdasarkan proses tersebut, praktik terbaik SOC yang diperoleh dari empat negara berjumlah 42 aktivitas dengan 7 kapabilitas yang diselenggarakan. Kapabilitas *Incident Triage, Analysis, and Response* terdiri dari 9 aktivitas; *CTI, Hunting, and Analysis* terdiri dari 5 aktivitas; *Expanded SOC Operation* terdiri dari 3 aktivitas; *Vulnerability Management* terdiri dari lima aktivitas; *SOC Tools, Architecture, and Engineering* terdiri dari 6 aktivitas; *Situational Awareness, Communication, and Training* terdiri dari 8 aktivitas; dan *Leadership and Management* terdiri dari 6 aktivitas.

Kapabilitas dan aktivitas yang dijalankan NSOC di Indonesia dijelaskan dalam dokumen Grand Desain NSOC [43]. NSOC memiliki 9 kapabilitas dan 42 aktivitas dengan rincian yang disajikan pada Tabel 2.

Tabel 2. Kapabilitas dan Aktivitas yang diselenggarakan NSOC

SOC Capability	Aktivitas
Monitoring	1. Penyelenggaraan Monitoring Anomali Trafik. 2. Penyusunan laporan anomali trafik yang berkaitan dengan stakeholder. 3. Penyusunan laporan situasional keamanan siber dan situational awareness tahunan. 4. Mengkomunikasikan hasil pemantauan anomali kepada *stakeholder.* 5. Mengelola dokumentasi aset informasi cakupan monitoring. 6. Melakukan pemeriksaan status pengiriman *log* keamanan dan kondisis sistem monitoring. 7. Menyelenggarakan penelusuran hasil deteksi monitoring. 8. Memberikan asistensi penyelenggaraan monitoring. 9. Menyusun dokumen standar, prosedur, dan kebijakan yang diperlukan dalam menunjang layanan monitoring. 10. Menyusun publikasi praktik terbaik dalam penyelenggaraan monitoring.
Cyber Threat Intelligence	1. Penyelenggaraan Layanan *Threat Intelligence.* 2. Penyelenggaraan Layanan dukungan informasi kejahatan siber untuk keperluan penegakan hukum. 3. Penyelenggaraan *Intelligence Information Gathering* dan melakukan pemetaan, dan pengolahan *Intelligence Information.* 4. Penyelenggaraan Analisis isu dan/atau tren keamanan siber.
IT Security Aseesment	1. Melakukan verifikasi terhadap kemungkinan upaya penerobosan keamanan infrastruktur dari perspektif eksternal. 2. Melakukan penilaian tingkat keamanan aplikasi. 3. Melakukan penilaian kerentanan berdasarkan tingkat ancaman, potensi kerugian, dan kemungkinan eksploitasi. 4. Memberikan rekomendasi umum terhadap kerentanan yang teridentifikasi pada aset.
Proteksi	1. Penyelenggaraan asistensi proteksi perbaikan kerentanan pada sistem elektronik. 2. Melakukan verifikasi perbaikan sistem elektronik setelah pelaksanaan ITSA. 3. Penyelenggaraan pemantauan, analisis, dan validasi aktivitas berbahaya pada sensor keamanan berbasis *endpoint.* 4. Penyusunan dokumen imbauan keamanan. 5. Penyelenggaraan penguaran keamanan pada sistem elektronik.
Pengelolaan Infrastruktur	1. Pemantauan ketersediaan dan kinerja infrastruktur TI dan *tools* yang digunakan dalam penyelenggaraan NSOC. 2. Penyelenggaraan pengelolaan seluruh aset NSOC .

p-ISSN: 2775-4227
e-ISSN: 2775-4219

SOC Capability	Aktivitas
	3. Penyelenggaraan evaluasi kontrol akses fisik yang diberikan kepada personel NSOC. 4. Pendokumentasian implementasi kontrol keamanan pada perangkat yang digunakan pada NSOC.
Threat Hunting	1. Penyelenggaraan layanan threat hunting pada *stakeholder*, sektor, dan nasional. 2. Penyelenggaraan *compromise assessment* pada aset terdampak serangan siber. 3. Penyelenggataan pengembangan dan sensor monitoring berbasis *open sources.* 4. Penyelenggaraan *rules management.*
Incident Response	1. Penyelenggaraan Pelaporan Insiden Siber dan *Incident Management*. 2. Penyelenggaraan validasi Registrasi Tim Tanggap Insiden Siber (CSIRT). 3. Penyelenggaraan komunikasi dengan stakeholder dalam rangka asistensi penanganan insiden. 4. Membangun komunikasi dengan mitra dari negara lain (CSIRT negara lain).
Forensik Digital	1. Penyelenggaraan layanan penyidikan insiden siber 2. Penyelenggaraan layanan bantuan investigasi bukti digital yang berkaitan dengan kejahatan siber, pelanggaran data, atau insiden lain yang melibatkan teknologi 3. Menjaga validitas dan intregritas pemeriksaan forensik digital
Analisis Malware	1. Penyelenggaraan layanan *honeynet* 2. Penyelenggaraan analisis *malware* 3. Penyelenggaraan pemasangan perangkat *honeypot* 4. Penyelenggaraan pengembangan sumber daya mitra yang bergabung dalam layanan *honeynet*

Aktivitas NSOC yang telah teridentifikasi pada Tabel 2 selanjutnya dibandingkan dengan praktik kapabilitas dan aktivitas terbaik SOC dari empat negara. Hal ini bertujuan untuk mengetahui kapabilitas maupun aktivitas yang belum dimiliki oleh NSOC. Hasil dari perbandingan disajikan dalam bentuk tabel dengan indikator "V" jika aktivitas sudah diselenggarakan oleh SOC dan indikator "X" jika aktivitas belum diselenggarakan oleh SOC. Berikut merupakan hasil perbandingan antara praktik terbaik aktivitas SOC dan aktivitas penyelenggaraan NSOC.

Tabel 3. Perbandingan Praktik Aktivitas Terbaik SOC dengan Aktivitas yang diselenggarakan NSOC

Kapabilitas SOC	Aktivitas	Ketersediaan Kapabilitas pada NSOC
Incident Triage, Analysis, and Response	1. Penyelenggaraan Layanan Pelaporan Insiden Siber.	✓
	2. Penyelenggaraan Layanan Asistensi Penanganan Insiden Siber.	✓
	3. Pelaksanaan Triase, Investigasi, dan Analisis Insiden Siber.	✓
	4. Penyusunan Panduan dan Regulasi Penanganan Insiden Siber.	✓
	5. Penyelenggaraan Mitigasi dan Pemulihan Insiden Siber.	✓
	6. Pengeloaan Log sebagai Bukti Investigasi Insiden Siber.	✓
	7. Penyelenggaraan Monitoring Ancaman Siber selama 24/7.	✓
	8. Penyusunan Playbook untuk Penanganan Insiden Siber Tertentu.	✓
	9. Penyusunan Dokumen Perencanaan Penyelenggaraan Layanan Respons Insiden.	✓
CTI, Hunting, and Analytics	1. Penyelenggaraan Layanan *Threat Hunting* sebagai metode deteksi ancaman tersembunyi.	✓
	2. Pengembangan *tools* deteksi berbasis *use-case* hasil analisis terhadap anomali yang terdeteksi.	✓
	3. Penyelenggaraan layanan *threat intelligence.*	✓
	4. Penyelenggaraan koordinasi pemantauan ancaman siber dengan mitra internasional.	✓
	5. Penyelenggaraan *Threat Intelligence Sharing*.	✓
Expanded SOC Operations	1. Penyelenggaraan Reviu dan Pengujian Kapabilitas Teknologi yang digunakan dalam Penanganan Siber.	✓

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Kapabilitas SOC		Aktivitas	Ketersediaan Kapabilitas pada NSOC
	2.	Pelaksanaan Publikasi Panduan Penyelenggaraan Simulasi Ancaman Siber.	×
	3.	Pelaksanaan Publikasi Panduan Penanganan *Insider Threat.*	×
Vulnerability Management	1.	Penyelenggaraan layanan *vulnerability management.*	×
	2.	Pelaksanaan publikasi panduan penilaian kerentanan dan penyelenggaraan *vulnerability management.*	×
	3.	Penyelenggaraan pemetaan aset, peran/fungsi aset, aliran data dari aset, dan perilaku pengguna aset.	✓
	4.	Penentuan skala prioritas aset dan potensi ancaman terhadap aset beserta dampak dari ancaman.	✓
	5.	Pelaksanaan publikasi panduan pengelolaan *patching* untuk aplikasi dan sistem operasi.	✓
SOC Tools, Architecture, and Engineering	1.	Implementasi otomatisasi pada proses *ticketing* insiden, *routing intelligence information*, dan distribusi alert/buletin.	×
	2.	Pengembangan *use-case* dan rules deteksi berdasarkan anomali trafik dan analisis terhadap *log*.	✓
	3.	Implementasi pencadangan server yang digunakan dalam penyelenggaraan SOC untuk menjaga ketersediaan layanan dan *backup* untuk proses pemulihan layanan jika terjadi insiden siber.	✓
	4.	Implementasi segmentasi jaringan internal SOC.	✓
	5.	Pelaksanaan publikasi panduan untuk mendesain infrastruktur jaringan yang aman.	✓
	6.	Penyelenggaraan layanan kerjasama pengembangan pengamanan ancaman siber.	✓
Situational Awareness, Communications, and Training	1.	Penyelenggaraan pelatihan dan pengembangan keterampilan personel SOC sesuai peran yang dilakukan.	✓
	2.	Pelaksanaan publikasi alert, buletin, dan informasi ancaman siber.	✓
	3.	Penyelenggaraan *cybersecurity exercise* berbasis skenario nyata untuk meningkatkan kesiapsiagaan dalam respons insiden siber.	✓
	4.	Penyelenggaraan komunikasi dan kerjasama dengan stakeholder, konstituen, dan mitra SOC terkait penanganan insiden siber.	✓
	5.	Penyelenggaraan pembangunan CSIRT untuk penanganan insiden.	✓
	6.	Penyusunan peta karir dan kompetensi personel SOC.	✓
	7.	Penyelenggaraan mekanisme *transfer knowledge* antar personel SOC.	×
	8.	Pelaksanaan publikasi panduan komunikasi bagi SOC, stakeholder, maupun konstituen ketika terjadi insiden siber dan fase pemulihan pasca insiden.	✓
Leadership and Management	1.	Penyusunan dokumen perencanaan dan pengelolaan SOC.	×
	2.	Penyelenggaraan reviu dan evaluasi penyelenggaraan SOC secara berkala.	×
	3.	Pelaksanaan publikasi panduan kebijakan peningkatan keamanan siber dan penanganan insiden bagi pimpinan organisasi/instansi.	×
	4.	Penyelenggaraan menajemen risiko keamanan siber.	✓
	5.	Penyelenggaraan publikasi panduan penyelenggaraan layanan manajemen risiko keamanan siber.	×

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Kapabilitas SOC	Aktivitas	Ketersediaan Kapabilitas pada NSOC
	6. Penyusunan dokumen perencanaan peningkatan SOC.	×

3.3. Rekomendasi Peningkatan NSOC di Indonesia

Rekomendasi peningkatan NSOC disusun berdasarkan hasil perbandingan praktik aktivitas terbaik SOC dengan aktivitas yang diselenggarakan NSOC yang telah disajikan pada Tabel 3. Rekomendasi peningkatan NSOC yang dapat dilakukan ialah sebagai berikut.

a. Penambahan aktivitas pada kapabilitas yang sudah tersedia NSOC diantaranya sebagai berikut.
   1) Kapabilitas *Expanded SOC Operations* membutuhkan penambahan aktivitas Penyusunan Panduan Penyelenggaraan Simulasi Ancaman Siber dan Panduan Penanganan *Insider Threat*.
   2) Kapabilitas *Vulnerability Management* membutuhkan penambahan aktivitas penyelenggaraan layanan *vulnerability management* dan penyusunan panduan penilaian kerentanan dan penyelenggaraan *vulnerability management.*
   3) Kapabilitas *SOC Tools, Architecture, and Engineering* membutuhkan penambahan aktivitas implementasi otomatisasi pada proses *ticketing* insiden, *routing intelligence information*, dan distribusi *alert*/bulletin.
   4) Kapabilitas *Situational Awareness, Communications, and Training* membutuhkan penambahan aktivitas penyelenggaraan mekanisme transfer *knowledge* antar personel SOC.

b. Penambahan Penambahan kapabilitas baru yang belum tersedia pada NSOC, yaitu kapabilitas *Leadership and Management*, perlu dilakukan sebagai bagian dari upaya penguatan fungsi strategis dan tata kelola. Meskipun salah satu aktivitas yang termasuk dalam kapabilitas *Leadership and Management* telah dijalankan oleh NSOC, namun pembentukan kapabilitas ini secara formal tetap diperlukan untuk memastikan keberlangsungan dan efektivitas fungsi tersebut. Penambahan kapabilitas ini dapat diwujudkan melalui pembentukan *role* atau tim khusus yang secara khusus bertanggung jawab atas penyelenggaraan aktivitas dalam kapabilitas tersebut. Pembentukan *role* khusus dimaksudkan agar penyelenggaraan kapabilitas dapat dilakukan dengan fokus dan memperoleh sudut pandang yang objektif. Kebutuhan akan objektivitas ini sangat penting, mengingat salah satu aktivitas utama dalam kapabilitas *Leadership and Management* adalah pelaksanaan reviu dan evaluasi terhadap kinerja SOC. Dengan demikian, penambahan kapabilitas ini diharapkan dapat mendukung penguatan tata kelola internal, meningkatkan akuntabilitas operasional, serta mendorong perbaikan berkelanjutan dalam pelaksanaan fungsi SOC di tingkat nasional.

3.4. Diskusi Dampak

Penelitian ini menekankan pentingnya pemahaman yang komprehensif mengenai peran dan aktivitas NSOC sebagai komponen fundamental keamanan siber nasional. Dengan melakukan pendekatan analisis literatur terhadap berbagai model dan strategi dari berbagai negara mengenai SOC, penelitian ini memberikan *gap* pelaksanaan dan landasan awal yang relevan bagi perumusan kebijakan serta pengembangan kerangka kerja NSOC di Indonesia. Hasil kajian ini dalam jangka pendek berpotensi menjadi acuan dalam penguatan struktur organisasi dan tata kelola NSOC yang lebih adaptif terhadap perkembangan ancaman siber yang dinamis bagi BSSN selaku penanggung jawab NSOC. Sedangkan untuk jangka panjang, penelitian ini dapat mendorong adanya integrasi yang lebih kuat antara NSOC dengan ekosistem keamanan siber nasional yang dapat berasal dari sektor pemerintahan, industri, dan akademisi. Penelitian ini juga membuka ruang eksplorasi lebih lanjut melalui studi empirik terhadap implementasi strategi NSOC di Indonesia maupun dalam pengembangan model kapabilitas dan aktivitas NSOC yang disesuaikan dengan konteks tantangan dan sumber daya nasional.

4. KESIMPULAN

4.1. Kesimpulan

Penelitian merekomendasikan penambahan sembilan aktivitas dan satu kapabilitas baru yang dapat diimplementasikan oleh NSOC di Indonesia. Rekomendasi tersebut diperoleh melalui proses perbandingan antara praktik terbaik kapabilitas dan aktivitas SOC dari negara lain dengan kapabilitas dan aktivitas yang saat ini telah dijalankan oleh NSOC. Penentuan kapabilitas dan aktivitas terbaik dilakukan melalui studi literatur, analisis, pemetaan , dan generalisasi terhadap panduan resmi yang diterbitkan oleh empat negara, yaitu Uni Eropa, Inggris,

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Amerika Serikat, dan Australia. Hasil dari proses tersebut mengidentifikasi tujuh kapabilitas utama yang terdiri dari 42 aktivitas sebagai praktik terbaik dalam penyelenggaraan SOC.

Hasil penelitian ini dapat digunakan oleh perumus kebijakan penyelenggaraan NSOC sebagai acuan awal upaya peningkatan kapabilitas dan aktivitas yang diselenggarakan. Dalam rangka mengimplementasikan rekomendasi yang telah disusun, NSOC dapat mengadopsi standar dan *framework* internasional seperti NIST atau ISO. Penggunaan standar dan *framework* tersebut diharapkan dapat memberikan acuan yang terstruktur, sehingga pelaksanaan rekomendasi menjadi lebih terstandardisasi dan optimal.

4.2. Rekomendasi Penelitian Selanjutnya

Terdapat beberapa usulan untuk penelitian lanjutan. Pertama, eksplorasi lebih teknis terhadap langkah-langkah yang implementatif untuk melaksanakan rekomendasi yang dihasilkan dalam penelitian ini. Kedua, pengujian terhadap hasil *benchmarking* kapabilitas dan aktivitas SOC melalui pendekatan *expert judgement*, untuk memperoleh masukan yang lebih mendalam serta validasi terhadap penetapan kapabilitas dan aktivitas terbaik yang relevan dengan implementasi SOC secara efektif.

DAFTAR PUSTAKA

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[2] Asosiasi Penyedia Jasa Internet Indonesia, "Profil Internet Indonesia 2022," Jakarta, 2022. Accessed: May 15, 2025. [Online]. Available: https://apjii.or.id/survei2019x/download/E17NsDYZ5pj0Wd32CqFGQfJRlA4vSV

[3] Asosiasi Penyelenggara Jasa Internet Indonesia, "Survei Penetrasi Internet Indonesia 2024," Jakarta, Feb. 2024. Accessed: May 15, 2025. [Online]. Available: https://survei1.apjii.or.id/download_survei/0c552657-97e4-4065-9f31-cbd0f809be82

[4] T. Oluwaseun Abrahams, S. Kuzankah Ewuga, S. Onimisi Dawodu, A. Oluwatoyin Adegbite, and A. Olanipekun Hassan, "A Review of Cybersecurity Strategies in Modern Organizations: Examining The Evolution and Effectiveness of Cybersecurity Measures for Data Protection," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 1–25, 2024, doi: 10.51594/csitrj.v5i.699.

[5] J. Rahman *et al.*, *Laporan Tahunan Monitoring Keamanan Siber 2021*, 1st ed. Jakarta: Badan Siber dan Sandi Negara, 2022.

[6] Pusat Operasi Keamanan Siber, *Laporan Tahunan Monitoring Keamanan Siber 2020*. Badan Siber dan Sandi Negara, 2021.

[7] Direktorat Operasi Keamanan Siber, *Lanskap Keamanan Siber Indonesia 2022*. Jakarta: Badan Siber dan Sandi Negara, 2023.

[8] Direktorat Operasi Keamanan Siber, *Lanskap Keamanan Siber Indonesia 2023*. Jakarta: Badan Siber dan Sandi Negara, 2024. Accessed: May 15, 2025. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[9] Direktorat Operasi Keamanan Siber, *Lanskap Keamanan Siber Indonesia 2024*. Jakarta: Badan Siber dan Sandi Negara, 2025. Accessed: May 15, 2025. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.pdf

[10] Republik Indonesia, "Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara," Jakarta, 2021. Accessed: May 15, 2025. [Online]. Available: https://peraturan.bpk.go.id/Details/165493/perpres-no-28-tahun-2021

[11] Badan Siber dan Sandi Negara, "Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara," Jakarta, 2020. Accessed: May 15, 2025. [Online]. Available: https://peraturan.bpk.go.id/Details/174286/peraturan-bssn-no-9-tahun-2020

[12] Badan Siber dan Sandi Negara, "Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara," Jakarta, 2021. Accessed: May 15, 2025. [Online]. Available: https://peraturan.bpk.go.id/Details/174277/peraturan-bssn-no-6-tahun-2021

[13] Badan Siber dan Sandi Negara, "Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2021 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020 - 2024," 2021. Accessed: May 15, 2025. [Online]. Available: https://peraturan.bpk.go.id/Details/226095/peraturan-bssn-no-10-tahun-2021

[14] K. Knerler, I. Parker, and C. Zimmerman, *11 Strategies of a World-Class Cybersecurity Operations Center*, 2nd ed. The MITRE Corporation, 2022. Accessed: May 15, 2025. [Online]. Available:

p-ISSN: 2775-4227
e-ISSN: 2775-4219

https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf
[15] E. Taurins, "How To Setup Up CSIRT and SOC," Dec. 2020. doi: 10.2824/056764.
[16] Cybersecurity & Infrastructure Security Agency, "Security Operations Center as a Service (SOCaaS)," https://www.cisa.gov/resources-tools/services/security-operations-center-service-socaas. Accessed: May 15, 2025. [Online]. Available: https://www.cisa.gov/resources-tools/services/security-operations-center-service-socaas
[17] A. Dedeke and K. Masterson, "Contrasting cybersecurity implementation frameworks (CIF) from three countries," *Information and Computer Security*, vol. 27, no. 3, pp. 373–392, Jun. 2019, doi: 10.1108/ICS-10-2018-0122.
[18] M. A. Ulin Nuha, Muhammad Salman, Nur Annisa Kadarwati Febriyani, and Eka Hero Ramadhani, "Reformulation of the Vulnerability Management Cycle for Enhancing Indonesia's Critical Information Infrastructure Protection: An International Comparative Study," *The Indonesian Journal of Computer Science*, vol. 14, no. 1, pp. 322–337, Feb. 2025, doi: 10.33022/ijcs.v14i1.4609.
[19] V. Kravets, "Comparative Analysis of the Cybersecurity Indices and Their Applications," *Theoretical and Applied Cybersecurity*, vol. 1, no. 1, May 2019, doi: 10.20535/tacs.2664-29132019.1.169090.
[20] H. Yarovenko, O. Kuzmenko, and M. Stumpo, "Strategy for Determining Country Ranking by Level of Cybersecurity," *Financial Markets, Institutions and Risks*, vol. 4, no. 3, pp. 124–137, 2020, doi: 10.21272/fmir.4(3).124-137.2020.
[21] M. Alfano, V. Bastidas, P. Heynen, and M. Helfert, "An Assessment Methodology and Instrument for Cybersecurity: The Ireland Use Case," Feb. 2023, [Online]. Available: http://arxiv.org/abs/2302.05166
[22] A. Niedermeier, "Same threat, different answers? Comparing and assessing national cyber defence strategies in Central-Eastern Europe," *Security and Defence Quarterly*, vol. 16, no. 3, pp. 52–74, Sep. 2017, doi: 10.35467/sdq/103184.
[23] International Telecommunication Union, "Global Cybersecurity Index 2024 5th Edition Acknowledgements," 2024. Accessed: May 15, 2025. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx
[24] ACSC, "Practical cyber security tips for business leaders," Canberra, Jan. 2024. Accessed: May 15, 2025. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2025-03/Practical%20cybersecurity%20tips%20for%20business%20leaders%20%28January%202024%29.pdf
[25] ACSC, *Information Security Manual*. Canberra: Australian Cyber Security Centre, 2024. Accessed: Dec. 28, 2024. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2024-12/Information%20Security%20Manual%20%28December%202024%29.pdf
[26] ACSC, "Essential Eight Maturity Model," Canberra, Nov. 2023. Accessed: May 15, 2025. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2025-03/Essential%20Eight%20maturity%20model%20%28November%202023%29.pdf
[27] ACSC, "ASD Cyber Threat Report 2023-2024," 2024. Accessed: May 15, 2025. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2024-11/asd-cyber-threat-report-2024.pdf
[28] National Cyber Security Centre, "Building a Security Operations Centre (SOC)." Accessed: May 15, 2025. [Online]. Available: https://www.ncsc.gov.uk/collection/building-a-security-operations-centre
[29] National Cyber Security Centre, "Introduction to Logging for Security Purposes : Laying the groundwork for incident readiness." Accessed: May 15, 2025. [Online]. Available: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes
[30] United Kingdom Government, "Detecting the Unknown: A Guide to Threat Hunting," Mar. 2019. Accessed: May 15, 2025. [Online]. Available: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Detecting-the-Unknown-A-Guide-to-Threat-Hunting-v2.0.pdf
[31] United Kingdom Government, "Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts version 2.0," Mar. 2019. Accessed: May 15, 2025. [Online]. Available: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf
[32] National Cyber Security Centre United Kingdom, "CISP : Connect Inform Share Protect." Accessed: May 15, 2025. [Online]. Available: https://www.ncsc.gov.uk/cisp/home
[33] National Cyber Security Centre United Kingdom, "Report a Cyber Incident." Accessed: May 15, 2025. [Online]. Available: https://report.ncsc.gov.uk/?_gl=1*affn63*_ga*MTAyNjY0NjUwMy4xNzQ0OTMxMDE1*_ga_FMH2FBTCEP*czE3NDcyMjQxNzEkbzI5JGcxJHQxNzQ3MjI2MTEzJGowJGwwJGgxNTg0NDk2NzI.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

[34] National Cyber Security Centre United Kingdom, "Incident management: How to effectively detect, respond to and resolve cyber incidents." Accessed: May 15, 2025. [Online]. Available: https://www.ncsc.gov.uk/collection/incident-management
[35] National Cyber Security Centre United Kingdom, "Exercise in a Box." Accessed: May 15, 2025. [Online]. Available: https://www.ncsc.gov.uk/section/exercise-in-a-box/overview
[36] Carneige Mellon University, "CRR Supplemental Resource Guide Asset Management," 2016. Accessed: May 15, 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-AM.pdf
[37] Carneige Mellon University, "CRR Supplemental Resource Guide, Volume 2: Controls Management," 2016. Accessed: May 15, 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-CM_0.pdf
[38] Carneige Mellon University, "CRR Supplemental Resource Guide Vulnerability Management Version 1.1," 2016. Accessed: May 15, 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf
[39] Carneige Mellon University, "CRR Supplemental Resource Guide, Volume 10: Situational Awareness," 2016. Accessed: May 15, 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-SA_0.pdf
[40] Cybersecurity & Infrastructure Security Agency, "Cyber Threat Information Sharing (CTIS) - Shared Cybersecurity Services (SCS)." Accessed: May 15, 2025. [Online]. Available: https://www.cisa.gov/resources-tools/services/cyber-threat-information-sharing-ctis-shared-cybersecurity-services-scs
[41] Cybersecurity & Infrastructure Security Agency, "Cyber Incident Resource Guide for Governors," 2023. Accessed: May 15, 2025. [Online]. Available: https://csrc.nist.gov/glossary/term/incident
[42] Carneige Mellon University, "CRR Supplemental Resource Guide, Volume 5: Incident Management," 2016. Accessed: May 15, 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-IM_0.pdf
[43] Pusat Operasi Keamanan Siber Nasional, *Grand Desain NSOC - National Security Operation Center*. Jakarta: BSSN, 2021.