Analisis Kemampuan *Security Incident Response* PT. XXX dalam Mengelola Insiden Siber

Monica Christy Natalia[1)], Rheva Anindya Wijayanti [2)]
1) Badan Siber dan Sandi Negara, monica.christy@bssn.go.id
2) Politeknik Siber dan Sandi Negara, rheva.anindya@student.poltekssn.ac.id

Abstrak

Penelitian ini merupakan studi pustaka terkait analisis kemampuan Security Operations Center (SOC) dalam mengelola insiden siber dimana berdasarkan hasil pemantauan anomali trafik terhadap Indonesia mulai 1 Januari 2021 pukul 00:00:00 hingga 31 Desember 2021 pukul 23:59:59 oleh PT.XXX terdapat 1.637.973.022 anomali yang tergolong cukup banyak. Penelitian ini menggunakan pendekatan kualitatif dengan pengumpulan data melalui wawancara dan studi literatur yang bertujuan untuk menganalisis kemampuan SOC dalam mengelola insiden siber dan menganalisis kendala yang dialami SOC dalam mengelola insiden siber. Hasil dari penelitian ini adalah kemampuan SOC PT. XXX dari aspek people, process, dan technology sudah baik namun masih perlu ditingkatkan. Sedangkan jika ditinjau dari proses pengelolaan insiden siber yang masuk sebagai aduan siber, SOC PT. XXX menggunakan langkah langkah insiden respon berdasarkan NIST incident response lifecycle dan sudah dilakukan dengan cukup baik. Namun masih terdapat kendala terutama dari komponen people dimana kuantitas sumber daya manusia yang masih kurang sebagai analis SOC dan teknologi yang sudah memadai namun masih kurang jumlahnya untuk cakupan seluruh Indonesia.

Kata kunci: Analisis Kemampuan, Keamanan Siber, NIST CSF, SOC

Abstract

This research is a literature study related to the analysis of the capabilities of the Security Operations Center (SOC) in managing cyber incidents where based on the results of traffic anomaly monitoring of Indonesia from January 1, 2021 at 00:00:00 to December 31, 2021 at 23:59:59 by PT. XXX there are 1.637.973.022 anomalies which are quite a lot. This research uses a qualitative approach with data collection through interviews and literature studies which aims to analyze the ability of the SOC to manage cyber incidents and analyze the obstacles experienced by the SOC in managing cyber incidents. The results of this study are the ability of PT. XXX SOC from the aspects of people, process, and technology is good but still needs to be improved. Meanwhile, when viewed from the process of managing cyber incidents that enter as cyber complaints, the PT. XXX SOC uses the incident response steps based on the NIST incident response lifecycle and has been done quite well. However, there are still obstacles, especially from the people component where the quantity of human resources is still lacking as SOC analysts and technology is adequate but still lacking in number for coverage throughout Indonesia.

Keywords: Capability Analysis, Cyber Security, NIST CSF, SOC

1. PENDAHULUAN

Seiring dengan meningkatnya kemajuan internet di Indonesia, hampir seluruh lapisan masyarakat mengenal internet. Perkembangan internet juga diikuti dengan perkembangan teknologi informasi. Perkembangan internet dan teknologi informasi yang sangat pesat dapat membawa dampak yang baik dan juga buruk. Informasi yang didapat melalui internet dapat menjadi alat bantu dalam pengambilan keputusan hingga menjadi tren gaya hidup masyarakat modern. Namun juga menimbulkan insiden keamanan informasi yang terus meningkat tidak hanya meningkat dari sisi jumlah namun menjadi lebih beragam dan lebih merusak hingga bisa mengganggu ketersediaan layanan.

Berdasarkan hasil pemantauan anomali lalu lintas di dunia maya terhadap Indonesia mulai 1 Januari 2021 pukul 00:00:00 hingga 31 Desember 2021 pukul 23:59:59 oleh PT. XXX terdapat 1.637.973.022 anomali. Statistik anomali tertinggi terjadi pada bulan Desember 2021 dengan jumlah anomali mencapai 242.066.168. Anomali yang dideteksi melalui *monitoring* yang dilakukan, didapatkan alamat *Internet Protocol* (IP) sumber dan tujuan anomali. Alamat IP tersebut dapat menunjukkan dari negara manakah anomali berasal dan ke negara manakah anomali ditujukan. Beberapa alamat IP menunjukkan aktivitas anomali yang sangat masif hingga mencapai jutaan lalu lintas di dunia maya dalam kurun waktu satu bulan. Banyaknya jumlah anomali dalam waktu yang singkat dapat disebabkan oleh aktivitas zbot, trojan dan *malware* lainnya.

Penelitian Safa *et al*. [1] menyebutkan bahwa langkah-langkah teknis yang efektif mampu mencegah insiden keamanan informasi siber dari pelanggaran keamanan informasi. Kegiatan penanggulangan serangan siber dapat menggunakan pendekatan yang menyesuaikan dengan sumber dan bentuk serangan yang dihadapi. Bentuk penanggulangannya dapat berupa pertahanan siber, penanganan secara hukum dan serangan balik siber. Tujuan utama pertahanan siber adalah membangun kapasitas nasional dalam menciptakan ketahanan

terhadap berbagai ancaman siber dan meningkatkan keamanan aset informasi [2].

Kerentanan di dalam sistem jika tidak ditangani dengan benar, berpotensi menyebabkan serangkaian tindakan tidak sah. Sangat penting organisasi untuk memperlakukan setiap insiden siber dengan mengimplementasikan metode, mekanisme, dan/atau kebijakan respons yang tepat untuk meminimalkan efeknya. Penanggulangan ini dapat bervariasi dari perbaikan sederhana seperti pembaruan perangkat lunak hingga kebijakan. *Incident response* selalu menjadi aspek penting dari keamanan informasi. *Incident response* dapat didefinisikan sebagai proses yang bertujuan untuk meminimalkan kerusakan dari insiden keamanan dan malfungsi, serta memantau dan belajar dari insiden tersebut [3]. Mengembangkan dan menerapkan *incident response* akan membantu organisasi dalam menangani pelanggaran data dengan cepat efisien dan dengan meminimalkan kerusakan [4].

Salah satu solusi untuk dapat bertahan dari ancaman siber adalah menerapkan *Security Operation Center* (SOC) sehingga organisasi memiliki panduan dalam kesiapsiagaan, tanggapan, dan pemulihan terhadap insiden. SOC adalah suatu sistem yang berfungsi sebagai sistem pertahanan siber dimana dapat mengelola *vulnerability assessment*, insiden siber dan memprediksi kemungkinan ancaman siber. Tujuan dalam membangun SOC yaitu untuk melindungi aset dan data organisasi serta menjaga kredibilitas.

PT XXX memiliki tiga unit kerja yang memiliki fungsi untuk melakukan identifikasi dan proteksi, melakukan penanggulangan dan pemulihan, penanganan insiden siber, serta melakukan pengelolaan informasi dini ancaman serangan siber. Ketiga unit kerja ini saling berkoordinasi dan melaksanakan pemantauan, evaluasi, dan pelaporan di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, dan pemantauan insiden keamanan siber.

Tujuan penelitian ini yaitu mengkaji atau menilai proses dalam merespons insiden oleh SOC PT. XXX agar dapat digunakan untuk menganalisa dan menghadapi ancaman siber serta meletakkan dasar bagi manajemen pengetahuan *tacit* di organisasi untuk peningkatan efisiensi cara kerja dan proses dalam merespons insiden secara efisien dan sistematis.

2. LANDASAN TEORI

Bagian ini mencatumkan teori-teori yang berkaitan dengan penelitian, yaitu keamanan siber, SOC, analisis kemampuan, dan *National Institute of Standards and Technologies* (NIST) *Cyber Security Framework* (CSF).

2.1 Keamanan Siber

Istilah keamanan siber diadopsi secara luas selama tahun 2000. ISO mendefinisikan keamanan siber sebagai kerahasiaan, integritas dan ketersediaan informasi di ruang siber [5]. Sedangkan menurut IBM, keamanan siber adalah praktik melindungi sistem penting dan informasi sensitif dari serangan digital. Juga dikenal sebagai keamanan teknologi informasi (TI) yaitu tindakan keamanan siber yang dirancang untuk memerangi ancaman terhadap sistem dan aplikasi jaringan, baik ancaman tersebut berasal dari dalam atau luar organisasi [6]. Keamanan siber mengacu pada *International Communication Union* (ITU) yaitu kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan siber dan organisasi serta aset pengguna. Organisasi dan aset pengguna mencakup perangkat komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirim dan/atau disimpan di lingkungannya. Keamanan siber berusaha untuk memastikan pencapaian dan pemeliharaan properti keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan di lingkungan siber [7].

Keamanan siber memiliki kerangka kerja yang digunakan oleh praktisi industri untuk menilai risiko siber dan menentukan kematangan keamanan siber organisasi tersebut. Beberapa kerangka keamanan siber yang umum digunakan yaitu *National Institute of Standards and Technology* (NIST), *International Organization for Standardization* (ISO) 27001, *Control Objectives for Information and Related Technologies* (COBIT 5), *Cyber Security Capability Maturity Model* (C2M2) , *Capability Maturity Model Integration* (CMMI). Kemampuan untuk mendapatkan sudut pandang *end-to-end* pada postur kematangan siber akan memungkinkan manajemen membuat keputusan yang tepat atas investasi yang mereka lakukan untuk menerapkan langkah-langkah keamanan siber. Untuk melakukannya diperlukan kemampuan untuk menilai risiko dunia maya, menentukan tingkat kematangan keamanan dunia maya, dan menghitung pengembalian investasi keamanan perlu dimasukkan dalam kerangka *end-to-end*.

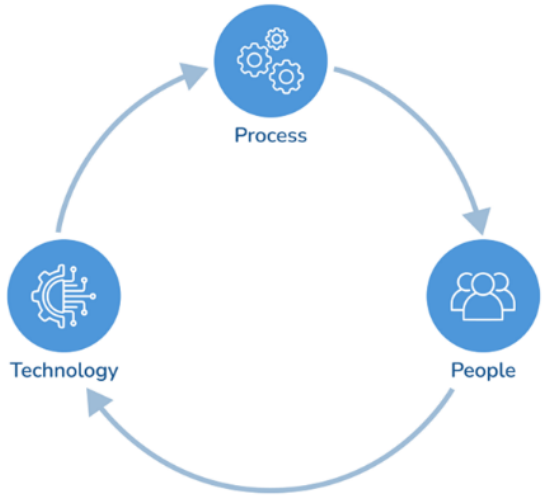
2.2 *Security Operation Center*

Security Operation Center (SOC) adalah inti dari operasi keamanan jaringan (sebagai bagian utama IoTI) yang bertujuan untuk memberikan perlindungan berkelanjutan, deteksi, dan kemampuan respons terhadap ancaman keamanan informasi, kerentanan perlindungan konstan dan berkelanjutan yang dapat dieksploitasi dari jarak jauh, dan insiden keamanan informasi *real-time* di jaringan. Pada awalnya SOC harus memiliki perangkat lunak dan perangkat keras yang diperlukan untuk merespons ancaman keamanan siber tingkat lanjut, untuk menganalisis internal, eksternal dan koneksi jaringan perimeter, untuk mendeteksi serangan tepat waktu bahkan bisa lebih

awal untuk menggagalkannya. Kedua, setiap SOC harus memiliki beberapa operator yang memasukkan analis data dan keamanan pada staf yang hanya berfokus pada analitik (jumlahnya bergantung pada ukuran dan kompleksitas IoTI) [8].

2.3 Analisis Kemampuan

Membangun SOC diperlukan beberapa pertimbangan kemampuan yang relevan terkait model operasi SOC selain layanan SOC (Muniz et al., 2016). SOC yang ideal bisa dikatakan memiliki semua kemampuan untuk mencapai, memenuhi atau melampaui efektivitas dari proses TI. Dalam membangun SOC yang efektif dan optimal harus memperhatikan komponen *people*, *process*, dan *technology*. Tiap komponen ini memiliki indikator yang selanjutnya dijabarkan dalam beberapa pertanyaan dan dapat memberikan gambaran terkait kemampuan suatu SOC. Berikut ini penjelasan dari masing-masing komponen tersebut yang diilustrasikan pada Gambar 1 [9] :



Gambar 1. Diagram kemampuan SOC

1. ***People***. Merupakan orang yang terlibat dalam SOC. Terdapat dua aspek yang perlu dipertimbangkan terkait komponen *people* pada SOC. Pertama, tiap orang dalam organisasi perlu menyadari peran dan tanggung jawabnya dalam mencegah dan mengurangi insiden atau ancaman siber. Kedua adalah tersedianya staf keamanan siber teknis khusus yang memiliki keterampilan dan kualifikasi untuk memastikan bahwa kontrol, teknologi, dan praktik dapat diterapkan untuk menangani ancaman siber tersebut.
2. ***Process***. *Process* adalah penghubung antara *people* dan *technology*. Keamanan proses operasi yang ingin dinilai berhubungan dengan bagaimana insiden keamanan dan kerentanan ditangani. Memahami dan mendokumentasikan keadaan proses SOC penting untuk pengembangan roadmap SOC yang sesuai dan realistis. Proses SOC dapat dikategorikan ke dalam beberapa tahap yakni triase insiden, pelaporan insiden, analisis insiden, penutupan insiden, aktivitas pasca insiden, penemuan kerentanan, dan remediasi dan pelacakan kerentanan.
3. ***Technology***. Mirip dengan *people* dan *process*, menggunakan teknologi yang tepat sangat penting untuk keberhasilan suatu SOC. Kategori teknologi yang harus dievaluasi yakni terkait kesiapan infrastruktur, pengumpulan dan pemrosesan *log*, pemantauan sistem, posisi kontrol keamanan, dan manajemen kerentanan.

2.4 National Institute of Standards and Technologies Cybersecurity Framework

National Institute of Standards and Technology (NIST) *Cybersecurity Framework* (CSF) [10] pertama kali diterbitkan di Amerika Serikat pada Februari 2014 sebagai tanggapan atas Perintah Eksekutif Presiden 1363 untuk membantu organisasi dalam meningkatkan keamanan siber pada infrastruktur kritis, manajemen risiko dan ketahanan sistem. *Framework* ini dapat meningkatkan keamanan siber infrastruktur kritikal guna menyelenggarakan aktivitas keamanan siber dasar pada tingkat tertinggi. CSF menawarkan konstruksi sederhana namun efektif yang terdiri dari tiga elemen yaitu *Core*, *Tiers*, dan *Profile*. *Core* merupakan seperangkat praktik keamanan siber, hasil dan kontrol keamanan teknis, operasional dan manajerial yang mendukung lima fungsi manajemen risiko yang terdiri dari *Identify*, *Protect*, *Detect*, *Respond*, dan *Recovery*. Ini berguna untuk mengelola risiko keamanan siber dengan mengatur informasi, mengaktifkan keputusan manajemen risiko, mengatasi ancaman, dan belajar dari aktivitas sebelumnya. *Tiers* menggambarkan kecakapan organisasi untuk mengelola risiko keamanan siber. Sedangkan *profile* adalah daftar hasil yang dipilih organisasi dari kategori dan subkategori berdasarkan kebutuhan dan penilaian risikonya. Berikut ini fungsi dan kategori CSF :

a. ***Identify***. Mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, aset, data, dan kemampuan. Kategorinya yaitu Manajemen Aset, Lingkungan Bisnis, Tata Kelola, Penilaian Risiko, Strategi Manajemen Risiko, Manajemen Risiko Rantai Pasokan.
b. ***Protect***. Mengembangkan dan menerapkan pengamanan yang sesuai untuk memastikan pengiriman layanan infrastruktur penting. Kategorinya yaitu Manajemen Identitas, Otentikasi dan Kontrol Akses, Kesadaran & Pelatihan, Keamanan Data, Perlindungan & Prosedur Informasi, Pemeliharaan, Teknologi Pelindung.
c. ***Detect***. Mengembangkan dan menerapkan aktivitas yang sesuai untuk mengidentifikasi terjadinya peristiwa keamanan siber. Kategorinya yaitu Anomali & Peristiwa, Pemantauan Keamanan Berkelanjutan, Proses Deteksi.
d. ***Respond***. Mengembangkan dan menerapkan

aktivitas yang sesuai untuk mengambil tindakan terkait peristiwa keamanan siber yang terdeteksi. Kategorinya adalah Perencanaan Respons, Komunikasi, Analisis, Mitigasi, Perbaikan.

e. ***Recover***. Mengembangkan dan mengimplementasikan aktivitas yang sesuai untuk mengambil tindakan terkait peristiwa keamanan siber yang terdeteksi. Kategorinya yaitu Perencanaan Respons, Perbaikan, Komunikasi

3. METODE PENELITIAN

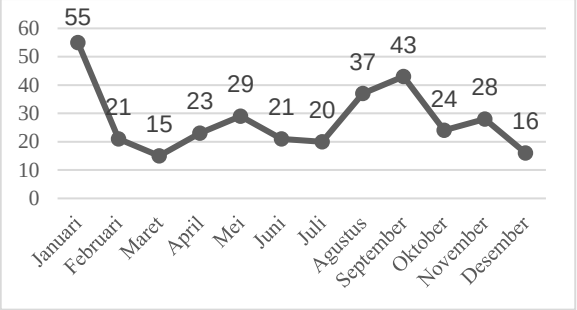
Penelitian ini dilakukan di Jakarta khususnya di PT. XXX sebagai lokus dari SOC, dilaksanakan pada Januari sampai dengan Februari 2023. Pada penelitian ini menggunakan pendekatan kualitatif deskriptif. Pendekatan kualitatif merupakan pendekatan untuk membangun pembangunan riil atas objek penelitian berdasarkan perspektif konstruktif (misalnya, makna-makna yang bersumber dari pengalaman individu, nilai- nilai sosial dan sejarah, dengan tujuan untuk mengembangkan teori atau pola pengetahuan tertentu), atau berdasarkan perspektif partisipatori (misalnya orientasi objek penelitian terhadap politik, isu, kolaborasi, atau perubahan) atau keduanya [11]. Penelitian kualitatif dapat digambarkan sebagai penelitian lapangan interaktif atau penelitian dokumenter non interaktif. Data dikumpulkan dengan pengamatan langsung di lapangan atau secara tidak langsung melalui jurnal, wawancara atau *focus groups*. Sedangkan proses pengumpulan data yang digunakan dalam penelitian ini adalah studi pustaka, wawancara, dan dokumentasi.

Narasumber dipilih berdasarkan pengetahuannya dan pengalamannya mengenai permasalahan dalam penelitian dan dapat dipercaya menjadi sumber data penelitian. Data yang telah diperoleh selanjutnya diproses dengan teknik triangulasi data untuk melakukan pemeriksaan keabsahan atau validitas data, selanjutnya dilakukan teknik analisis data dengan menggunakan reduksi data dan pada tahap akhir dilakukan penarikan kesimpulan.

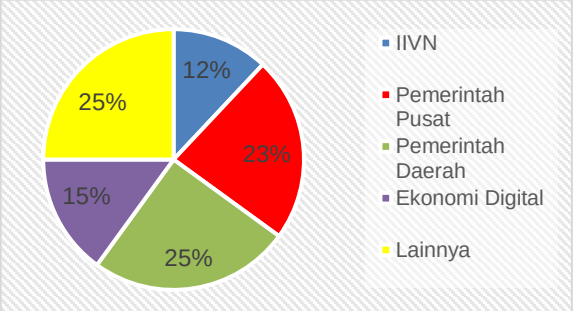
4. HASIL DAN PEMBAHASAN

4.1 Aduan Insiden Siber yang Diterima SOC PT.XXX

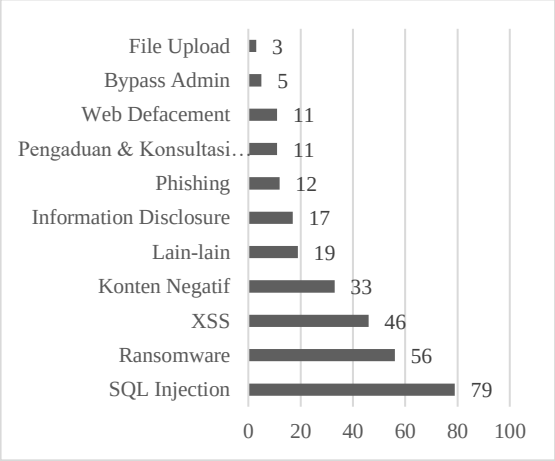
PT. XXX telah membangun SOC sejak tahun 2017 dan telah melakukan pemantauan terhadap berbagai anomali lalu lintas jaringan siber. Berdasarkan laporan tahunan monitoring keamanan siber 2021 terdapat 322 aduan siber di berbagai sebaran sektor di Indonesia yang dipantau oleh SOC PT. XXX seperti pada Gambar 2. Dimana aduan siber tertinggi terjadi pada bulan Januari 2021 dengan jumlah mencapai 55 aduan terkait serangan siber. Berikut merupakan tren aduan siber yang diterima SOC PT. XXX pada tahun 2021.



Gambar 2. Grafik tren aduan siber SOC PT. XXX 2021



Gambar 3. Grafik sebaran sektor aduan siber 2021



Gambar 4. Grafik sebaran jenis serangan pada aduan siber 2021

Dari data yang diterima SOC PT. XXX telah terjadi serangan siber pada berbagai sebaran sektor di Indonesia pada tahun 2021. Berdasarkan pada Gambar 3, sektor yang paling terdampak adalah pemerintah daerah sebesar 25% (81 aduan), sektor lainnya sebesar 25% (81 aduan), pemerintah pusat sebesar 23% (76 aduan), sektor ekonomi digital sebesar 15% (51 aduan), dan IIVN sebesar 12 % (43 aduan). Sedangkan tiga jenis aduan siber tertinggi yang dilaporkan berdasarkan jumlah kasus sesuai pembagian sektor yang diterima berdasarkan pada Gambar 4 yaitu SQL *Injection*, *Ransomware*, dan *Cross-Site Scripting* (XSS).

SQL *injection* adalah sebuah jenis injeksi berupa perintah SQL yang diinjeksikan ke dalam *data-plane input* untuk mempengaruhi eksekusi SQL *command* yang telah ditentukan. Ekploitasi SQL *injection* yang berhasil dapat melakukan pembacaan data sensitif dari *database*, mengubah data pada *database*,

menjalankan operasi administrasi pada *database*, dan dalam beberapa kasus mengeluarkan perintah ke sistem operasi. Serangan aduan siber tertinggi kedua adalah *ransomware*, yakni sebuah jenis *malware* yang menyerang korban dengan cara mengunci seluruh file yang dimiliki, meminta tebusan terhadap korban, dan penyerang akan memberikan kunci untuk digunakan korban dalam membuka dokumen yang dimiliki setelah korban membayar sesuai dengan tarif yang diberikan oleh penyerang. *Cross-Site Scripting* (XSS) adalah sebuah jenis injeksi berupa *script* berbahaya yang diinjeksikan ke sebuah situs rentan maupun terpercaya. Penyerang menggunakan aplikasi web untuk mengirim *malicious code*, umumnya dalam bentuk *browser side script* ke *end-user* berbeda. *Malicious script* dapat mengakses *cookie*, *session token*, ataupun informasi sensitif lainnya yang disimpan oleh *browser*. Hal ini menunjukkan bahwa serangan yang banyak terjadi di PT. XXX merupakan serangan dengan kategori tinggi dimana insiden yang terjadi berdampak parah pada operasi dan harus ditangani sesegera mungkin.

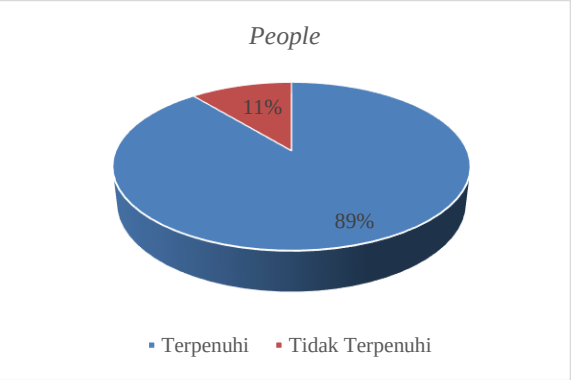
4.2 Analisis Kemampuan SOC PT. XXX

Saat ini jaringan informasi sebagai infrastruktur pertukaran informasi telah berkembang sangat pesat. Sayangnya perkembangan ini juga diikuti oleh pertambahan jumlah ancaman serangan siber. Untuk itu diperlukan solusi keamanan yang efektif dan relevan. SOC dapat melakukan korelasi antara informasi yang dikumpulkan dari berbagai solusi keamanan jaringan yang ada dan melakukan analisa terhadap insiden keamanan yang sedang terjadi [12].

Tabel 1. Indikator komponen *People*

No	Indikator
1	Verifikasi rekrutmen dan pengenalan analis level 1
2	Analis level 1 memiliki ruang kerja dan peralatan yang memadai
3	Analis level 1 telah divalidasi untuk memenuhi SLs
4	Penjadwalan *shift* untuk analis level 1 mencakup hingga akhir M1
5	Perhitungan ketersediaan kapasitas level 1 tambahan
6	Verifikasi rekrutmen dan pengenalan analis level 2
7	Analis level 2 memiliki ruang kerja dan peralatan yang memadai
8	Analis level 2 telah divalidasi untuk memenuhi SLs
9	Penjadwalan *shift* untuk analis Level 2 mencakup hingga akhir M1
10	Perhitungan ketersediaan level 2 tambahan
11	Materi pelatihan telah selesai dan ditinjau
12	Sesi pelatihan analis level 1 telah dijadwalkan dan diadakan
13	Sesi pelatihan analis level 2 telah dijadwalkan dan diadakan
14	*Recording sessions* tersedia untuk analis level 1 dan level 2
15	Materi *training* dipublikasikan
16	Informasi kontak untuk semua analis level 1 dan level 2
17	Grup analis IM disiapkan untuk semua analis
18	*Hotline* CSIRT ditambahkan ke profil telepon IP untuk analis SOC
19	Kemampuan telepon IP jarak jauh untuk analis SOC (opsional)

Dari data yang tertera pada Tabel 1 mengenai Analisis Kemampuan SOC PT. "XXX" berdasarkan komponen *people* dapat digambarkan pada diagram seperti pada Gambar 5.



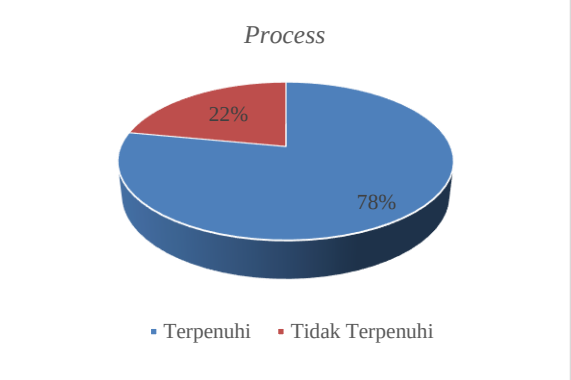
Gambar 5. Diagram komponen *People*

Gambar 5 menunjukkan diagram komponen *people* pada SOC PT. XXX sudah cukup baik, namun masih terkendala pada kuantitas sumber daya manusia.

Tabel 2. Indikator komponen *Process*

No	Indikator
1	Proses inti SOC terdokumentasi dan dikaji ulang
2	Analis level 1 dan 2 menerima pelatihan tentang semua proses inti SOC
3	Proses inti SOC telah dipublikasikan di wiki tim dan/atau basis pengetahuan
4	Prosedur inti SOC terdokumentasi dan dikaji ulang
5	Analis level 1 dan 2 menerima pelatihan tentang semua prosedur inti SOC
6	Prosedur inti SOC telah dipublikasikan di *team* wiki dan/atau SIEM *knowledge base*
7	Templat dokumen dan pelaporan SOC terdokumentasi dan dikaji ulang
8	Analis level 2 sudah menerima pelatihan tentang penggunaan templat dokumen dan pelaporan
9	Templat dokumen dan pelaporan SOC telah dipublikasikan di *team* wiki dan/atau SIEM *knowledge base*

Dari data yang tertera pada Tabel 2 mengenai Analisis Kemampuan SOC PT. XXX berdasarkan komponen *process* dapat digambarkan pada diagram seperti pada Gambar 6.



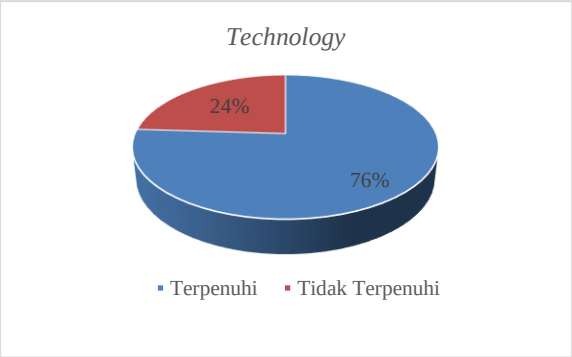
Gambar 6. Diagram komponen *Process*

Gambar 6 menunjukkan diagram komponen *process*. SOC PT. XXX masih terkendala pada komponen *process* yakni komunikasi.

Tabel 3. Indikator Komponen *Technology*

No	Indikator
1	Semua analis SOC memiliki peran dan izin dalam SIEM
2	*Live channel* untuk operator sudah terkonfigurasi
3	Notifikasi grup, tingkat eskalasi dan pengaturan tujuan sudah diatur dan divalidasi
4	Kasus penggunaan terinstal dan aturan korelasi divalidasi
5	SIEM *knowledge base* termasuk proses dan prosedur SOC
6	SIEM *knowledge base* menyertakan tautan untuk mendukung proses dan prosedur
7	Templat laporan sudah diatur dan dikonfigurasi dalam SIEM
8	Semua analis level 1 memiliki peran dan izin ke dalam sistem manajemen kasus/investigasi
9	Semua analis level 2 memiliki peran dan izin ke dalam sistem manajemen kasus/ penyelidikan
10	*Team* wiki diperbarui untuk menyertakan halaman manual dan instruksi tentang cara menggunakan sistem manajemen kasus/penyelidikan
11	Analisis level 1 dan 2 telah disiapkan dengan telepon individu dan ponsel
12	*Group teleconference bridges* sudah terpasang
13	*Instant messaging* dan *desktop video conferencing* telah diuji dan berfungsi
14	*Team* wiki dan/atau *knowledge base* telah diperbaharui dengan instruksi tentang cara menggunakan telepon dan sistem komunikasi
15	*Desktop dan video conferencing* telah terintegrasi dengan *video wall*
16	Analis level 2 memiliki peran dan izin ke dalam sistem *ticketing* IT
17	Antrean tiket SEC-CSIRT diatur dalam sistem *ticketing* TI dan analis SOC level 2 dapat mengakses antrian
18	Analis SOC level 2 telah menerima pelatihan manajer layanan dasar atau memiliki pengalaman manajer layanan sebelumnya
19	Analisis level 2 memiliki peran dan izin ke dalam platform wiki
20	Proses dan prosedur inti SOC diunggah ke wiki/*knowledge base*
21	Tautan ke proses dan prosedur pendukung telah diunggah ke wiki/ *knowledge ase*

Dari data yang tertera pada Tabel 3 mengenai Analisis Kemampuan SOC PT. XXX berdasarkan komponen *technology* dapat digambarkan pada diagram seperti pada Gambar 7.



Gambar 7. Diagram komponen *Technology*

Gambar 7 menunjukkan diagram komponen *technology* SOC PT. XXX yang saat ini sudah dapat memenuhi standar namun belum sepenuhnya dapat memenuhi cakupan seluruh Indonesia. Dari ketiga diagram di atas dapat dilihat bahwa kemampuan SOC PT. XXX sudah cukup baik komponennya namun perlu ditingkatkan.

Terdapat beberapa kendala SOC dalam mengelola insiden siber berdasarkan komponen pembangun SOC.

a. ***People***. Dalam suatu SOC hanya terdapat satu hingga dua orang analis per *shift* piket, namun SOC tersebut hanya dapat memantau instansi dalam jumlah sedikit yaitu sekitar satu hingga tiga instansi. SOC PT. XXX melakukan monitoring seluruh daerah di Indonesia, sehingga agak sulit untuk mendapatkan cakupan seluruh daerah baik dari segi biaya untuk pemasangan titik-titik sensor pemantauan maupun jumlah analis (satu tim piket terdiri dari enam orang analis untuk melakukan pemantauan seluruh Indonesia).
b. ***Process***. Selain dari komponen *people*, terdapat beberapa tantangan dari komponen *process*. Dalam mengelola insiden siber yang diterima tim insiden respon SOC PT. XXX terdapat kendala dalam komunikasi yaitu sudah tersedianya *team wiki* dan/atau SIEM *knowledge base* namun tidak pernah dipakai dan dimanfaatkan sehingga proses pengelolaan insiden siber masih menggunakan cara yang lebih konvensional.
c. ***Technology***. Tantangan yang dihadapi dalam membangun SOC dari komponen *technology* yaitu kompleksitas infrastruktur, dimana SOC PT. XXX sudah memiliki teknologi yang memadai namun masih kurang untuk cakupan seluruh Indonesia.

4.3 Analisis Proses Penanganan Insiden Siber SOC PT. XXX

Terdapat lima komponen yang perlu diperhatikan dalam menganalisis kemampuan sebuah SOC dalam menangani insiden siber yang masuk ke SOC PT. XXX yang efektif dan optimal yaitu *identify*, *protect*, *detect*, *respond*, dan *recover*. Dari data hasil penelitian dan wawancara narasumber, terdapat beberapa tantangan dalam membangun tim insiden respon sebuah SOC yang dapat mengelola aduan insiden siber dengan efektif dan optimal baik dari kelima komponen di atas.

Pada komponen *identify* terdapat indikator persiapan untuk penanganan insiden, pencegahan insiden, serta komunikasi dan pelaksanaan rencana. Pada komponen *protect* terdapat indikator pengenalan kemungkinan vektor serangan dan peninjauan sumber insiden yang memungkinkan. Pada komponen *detect* terdapat indikator penilaian awal dan penentuan prioritas langkah selanjutnya, pengumpulan barang bukti, dan komunikasi dengan pihak yang terkena

insiden. Pada komponen *respond* terdapat indikator pengembangan strategi penahanan, penghapusan ancaman, dan pengambilan langkah menuju pemulihan. Sedangkan pada komponen *recover* terdapat indikator pemantauan dan waspada.

Wawancara dilakukan pada bulan Januari tahun 2023 melalui media Telegram dengan beberapa narasumber dari PT. XXX. Relevansi narasumber dengan penelitian yaitu kemampuan dan pengalaman para narasumber yang dalam pekerjaannya bertanggung jawab dalam menggunakan sistem SOC. Menurut narasumber, tahapan pengelolaan insiden siber pada SOC PT. XXX sudah cukup baik. Berikut ini penjabaran tiap komponennya :

1. ***Identify***. Pada tahap ini, SOC PT. XXX melakukan persiapan untuk menangani atau mengelola insiden siber yang masuk. Namun bukan hanya mempersiapkan cara penanganan saat insiden terjadi namun juga melakukan pencegahan insiden dengan memastikan bahwa sistem, jaringan, dan aplikasi cukup aman.
2. ***Protect***. Pada tahap ini, SOC PT. XXX mengembangkan dan menerapkan perlindungan yang sesuai untuk memastikan layanan infrastruktur penting tetap terjaga walau insiden terjadi.
3. ***Detect***. Deteksi sebuah insiden merupakan tahapan untuk mengidentifikasi sebuah insiden dan memahami akibat dan tingkatannya. SOC PT. XXX akan mengamati anomali, melakukan pemantauan keamanan berkelanjutan dan proses deteksi.
4. ***Respond***. Ini adalah salah satu tahapan paling kritis dalam menangani insiden siber yang terjadi. Strategi penahanan dan pemulihan didasarkan pada informasi dan indikator kompromi yang dikumpulkan selama fase analisis. Ancaman perlu diberantas secara menyeluruh sebelum operasi normal dapat dilanjutkan untuk meminimalkan gangguan berulang berikutnya.
5. ***Recover***. Biasa disebut sebagai *post-incident review* dimana SOC PT. XXX secara proaktif meninjau rencana dan aktivitas respons insiden untuk mengidentifikasi dan mengatasi kekurangan serta memperkuat postur keamanan mereka.

5. KESIMPULAN

Berdasarkan analisis yang sudah dilakukan oleh peneliti tentang kemampuan SOC PT. XXX dalam mengelola insiden siber, dapat ditarik kesimpulan yaitu :

1. Dari hasil analisis kemampuan SOC PT. XXX dalam mengelola insiden siber, dapat dilihat bahwa kemampuan SOC PT. XXX cukup baik. Berdasarkan komponen *people*, *process*, dan *technology*, SOC PT. XXX sudah hampir memenuhi semua aspek yang diperlukan dalam membangun SOC yang efektif. Sedangkan jika ditinjau dari proses pengelolaan insiden siber yang masuk sebagai aduan siber, SOC PT. XXX menggunakan langkah-langkah insiden respon berdasarkan *NIST incident response lifecycle*. Setelah dianalisis menggunakan *framework* NIST CSF, semua langkah - langkah penangan insiden siber sudah dilakukan dengan cukup baik

2. Terdapat beberapa kendala dalam membangun SOC terutama dari segi komponen *people*. Faktor utama yang mempengaruhi komponen *people* yaitu dari kuantitas sumber daya manusia yang masih kurang sebagai analis SOC. Pada komponen *process*, SOC PT.XXX masih terkendala dalam penggunaan *team wiki* dan/atau SIEM *knowledge base* yang dapat mempermudah proses pengelolaan insiden siber namun tidak dimanfaatkan. Sedangkan pada komponen *technology*, SOC PT.XXX sudah memiliki teknologi yang memadai namun masih kurang untuk cakupan seluruh Indonesia.

   Terdapat beberapa saran yang dapat diimplementasikan baik untuk penelitian selanjutnya maupun *stakeholder*, antara lain :

   1. Meningkatkan jumlah atau kuantitas sumber daya manusia sebagai analis agar seluruh cakupan bagian di Indonesia dapat terakomodir.
   2. Mengupayakan pengadaan perangkat TI yang lebih banyak.
   3. Menggalakan kembali penggunaan *team wiki* dan/atau SIEM *knowledge base* untuk mempermudah pemantauan aktivitas jaringan.

REFERENSI

[1] N.S. Safa, R. Von Solms, and S. Furnell, “Information security policy compliance model in organizations,” *Comput Secur*, vol. 56, pp. 70–82, Feb. 2016, doi: 10.1016/J.COSE.2015.10.006.

[2] E. Suryadi, “Cyber defence sebagai garda terdepan ketahanan nasional,” *Share & Discover Presentations SlideShare*, April 2012. Accessed: Feb. 14, 2023. [Online]. Available: https://www.slideshare.net/EdiSuryadi1/cyber-defence-sebagai-garda-terdepan-ketahanan-nasional?from_action=save.

[3] J. H. P. Eloff and M. Eloff, “Information Security Management - A New Paradigm,” in SAICSIT ’03: the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through

technology, Sep. 2003, pp. 130–136.

[4] P. Mitropoulos, I. Mitropoulos, I. Giannikos, and A. Sissouras, "A biobjective model for the locational planning of hospitals and health centers," *Health Care Manag Sci*, vol. 9, no. 2, pp. 171–179, May 2006, doi: 10.1007/S10729-006-7664-9.

[5] "ISO - ISO/IEC 27032:2012 - Information technology — Security techniques — Guidelines for cybersecurity." Accessed: Feb. 14, 2023. [Online]. Available: https://www.iso.org/standard/44375.html

[6] "What is cybersecurity?," 27 October 2023. Accessed: Feb. 14, 2023. [Online]. Available: https://www.ibm.com/topics/cybersecurity

[7] International Telecommunication Union (2017). Global Cybersecurity Index 2017. International Telecommunication Unit.

[8] N. Miloslavskaya, "Security operations centers for information security incident management," *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, pp. 131–138, Sep. 2016, doi: 10.1109/FICLOUD.2016.26.

[9] J. Muniz, G. McIntyre, and N. AlFardan, "Security Operations Center Guidebook. A Practical Guide for a Successful SOC," *Indianapolis: Cisco Press*. 2016.

[10] M. Hyun, M. South, J. Mueller, "NIST Cybersecurity Framework (CSF)," *Amazon Web Services (AWS)*. Oct. 2021.

[11] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Fifth Edit. SAGE Publications, 2018.

[12] T. I. Digiserve, "SOC, Pusat Komando Sistem Pengamanan yang Ketat dan Berkelanjutan," *Digiserve*. Feb 2022. Diakses pada 14 Februari 2023 dari https://www.digiserve.co.id/id/insight/blog/soc-pusat-komando-sistem-pengamanan-yang-ketat-dan-berkelanjutan.