ETNIK : Jurnal Ekonomi – Teknik
ISSN: 2808-6694 (Online);2808-7291 (Print)
Jurnal Homepage https://etnik.rifainstitute.com

Perancangan Kapabilitas Security Operations Center (SOC): Studi Kasus PT XYZ

Muhammad Firzi Nabil[1], Setiyadi Yazid[2]

Universitas Indonesia

Informasi Artikel

Histori Artikel:
Submit ***10 September 2023***
Accepted ***15 September 2023***
Published ***20 September 2023***

Email Author:
FirziGT@gmail.com

ABSTRACT

Cybersecurity has become a major concern for organizations and companies around the world. PT XYZ is also very concerned about this aspect by implementing security policies in terms of governance and operations in their corporate initiatives.Unfortunately, the policy is less reflected for XYZ Group subsidiaries. The policies, frameworks, and workflows for cybersecurity have not been defined and structured so that they will be more vulnerable to the impact and risk of cyber-attacks and vulnerabilities compared to the parent company. Such risks include availability for applications, financial losses, internal and customer data leaks, and issues and fines from regulators. To avoid these risks, a Security Operations Center (SOC) for company group was created. The SOC is created so that the synergy or readiness for cybersecurity and its risk management for subsidiaries is equal to or exceeds that of the parent company. Some of the expected results and benefits are as a strategic initiative, increasing stakeholder trust, increasing security visibility, evaluating, and improving security, fulfilling regulations, closing security gaps, and increasing cybersecurity readiness. This research uses Soft System Methodology (SSM) with the NIST Framework. Data collection is in the form of observation, literature study, and interviews. The result of this research is an SOC capability design in the form of activities that need to be carried out and developed and prioritized. It is expected from the results of this research that the implementation of SOC in the group of companies will be effective and meet cybersecurity objectives.

Keyword– *Security Operations Center, Cybersecurity, Soft System Methodology*

ABSTRAK

Cybersecurity atau keamanan siber telah menjadi perhatian utama bagi organisasi dan perusahaan-perusahaan di seluruh dunia. Sebagai salah satu institusi perbankan terbesar di Indonesia, PT XYZ sangat memperhatikan aspek tersebut dengan menerapkan kebijakan keamanan dalam hal tata kelola dan operasional dalam

inisiatif perusahaan mereka.Sayangnya, kebijakan tersebut kurang tercermin untuk anak perusahaan dari PT XYZ. Kebijakan, kerangka, dan alur kerja untuk keamanan siber belum terdefinisikan dan terstruktur sehingga mereka akan lebih rentan terkena dampak dan risiko serangan dan kerentanan siber dibandingkan dengan perusahaan induk. Risiko tersebut termasuk *availaibility* untuk aplikasi, kerugian finansial, kebocoran data internal dan nasabah, dan masalah dan denda dari regulator.Untuk menghindari risiko tersebut, maka dibuatlah *Security Operations Center* (SOC) untuk grup perusahaan. SOC tersebut dibuat agar sinergi atau kesiapan untuk keamanan siber beserta manajemen risiko darinya bagi perusahaan anak lebih setara atau melebihi perusahaan induk. Tanggung jawab dan fungsi mereka mencerminkan kebijakan yang ada di perusahaan induk. Beberapa hasil dan manfaat yang diharapkan adalah sebagai inisiatif strategis, meningkatkan kepercayaan stakeholder, meningkatkan visibilitas keamanan, evaluasi dan peningkatan keamanan, pemenuhan regulasi, menutup celah keamanan, dan meningkatkan kesiapan keamanan siber. Penelitian ini menggunakan *Soft System Methodology* (SSM) dengan kerangka kerja NIST Framework. Pengumpulan data berbentuk observasi, studi literatur, dan wawancara. Hasil dari penelitian ini adalah rancangan kapabilitas SOC berupa aktivitas yang perlu dijalankan dan dikembangkan serta diprioritaskan. Diharapkan dari hasil penelitian ini agar penyelenggaraan SOC di grup perusahaan menjadi efektif serta memenuhi tujuan keamanan siber di lingkup grup perusahaan.

Kata Kunci – Pusat Operasi Keamanan, Kemanan Siber, Metodologi Soft System

PENDAHULUAN

Penggunaan Internet di Indonesia berkembang sangat pesat seiring waktu berjalan. Menurut Survei Internet APJII di tahun 2019-2020, jumlah pengguna internet di Indonesia di tahun 2019 meningkat menjadi 196,7 juta pengguna dengan tingkat penetrasi sebesar 73,7% dari jumlah Penduduk Indonesia (Asosiasi Penyelenggara Jasa Internet Indonesia, 2020). Berkembangnya penggunaan internet membuat posisi keamanan siber menjadi lebih penting. Salah satu dari risiko keamanan siber terebut adalah kebocoran atau pembobolan data. Di tahun 2020, kerugian rata-rata akibat dari pembobolan data secara global adalah sebesar 3,86 milliar Dollar Amerika. Kerugian tersebut termasuk biaya untuk menemukan dan merespon terhadap pembobolan tersebut, biaya downtime dan keuntungan yang hilang, dan kerusakan reputasi bagi organisasi yang terdampak (Mansfield-Devine, 2022).

Kerentanan siber terebut turut menjadi perhatian dari beberapa organisasi, salah satunya adalah PT XYZ. PT XYZ sebagai perusahaan induk mengoperasikan XYZ Group, yaitu sekelompok perusahaan dimana perusahaan induk tersebut membawahi beberapa perusahaan anak yang bergerak di berbagai bidang industri. Beberapa insiden kerentanan serangan siber telah terjadi di lingkup XYZ Group. Termasuk salah satu insiden terbesar dimana 2 (dua) juta data nasabah dari mereka dilaporkan bocor dan dijual di dark web. Meski pembobolan pada sistem anak perusahaan tersebut tidak menyebabkan gangguan sistem yang berarti di PT XYZ sebagai perusahaan induk, namun hal ini tentu saja dengan mudah mampu merusak reputasi tidak hanya

perusahaan tersebut, namun juga XYZ Group secara keseluruhan.

Secara umum, masalah keamanan yang dapat diamati termasuk respon keamanan yang kurang mencukupi untuk menghadapi tantangan serangan siber selanjutnya, khususnya dalam hal monitoring serta respons dan recovery secara tanggap dan tersetruktur. Selain itu, perusahaan anak sangat bergantung terhadap perusahaan induk tersebut yang berdampak padam penambahan beban kerja dan tanggung jawab bagi perusahaan induk. Selain itu, terdapat tuntutan regulasi yang berkembang seperti Peraturan OJK No.11/POJK.03/2022 dan POJK Nomor 38/POJK.03/2016 (Otoritas Jasa Keuangan, 2016; Otoritas Jasa Keuangan, 2022).

Oleh karena itu, PT XYZ perlu untuk melakukan cara-cara yang jauh lebih baik dalam pengelolaan sinergi cybersecurity di dalam XYZ Group. Pengelolaan keamanan siber tersebut dibutuhkan mengingat kesiapan untuk keamanan siber di perusahaan anak yang dinilai tertinggal dibandingkan perusahaan induk. Untuk itu, dibutuhkan Security Operations Center (SOC). Beberapa justifikasi mengenai pembuatan SOC tersebut dapat dijelaskan dari segi people, proses, dan teknologi. Dari segi people, pembentukan SOC dinilai dapat menyelesaikan tantangan untuk ketersediaan tenaga ahli keamanan siber yang masih sedikit dengan perekrutan, pelatihan, dan penjagaan tenaga ahli tersebut sehingga keahlian dan pengalaman mereka dapat menyamai perusahaan induk. Dari segi proses, SOC dinilai dapat membentuk kerangka kerja yang efisien dan efektif, baik secara tenaga maupun finansial. Diharapkan proses tersebut dapat lebih align dengan target keamanan siber yang diharapkan grup perusahaan secara keseluruhan. Secara teknologi, SOC diharapkan dapat menyeimbangkan ketersediaan infrastruktur teknologi yang ada di lingkup grup perusahaan sehingga dapat menyesuaikan sesuai kebutuhan dari keamanan siber mereka.

METODE

Metodologi penelitian ini menggunakan Soft System Methodology (SSM). SSM adalah salah satu metode penelitian metode kualitatif, yang mendefinisikan prinsip-prinsip untuk menggunakan metode yang memungkinkan intervensi dalam situasi masalah struktural yang dimana mempertahankan hubungan sama pentingnya dengan menemukan tujuan. Untuk menjawab pertanyaan tentang metodologi SSM dan apa yang dilakukan secara signifikan menentukan bagaimana melakukannya (Jackson, 2003).

Tahapan dari penelitian ini menggunakan SSM tersebut adalah sebagai berikut:

1. Identifikasi masalah yang dihadapi dalam manajemen keamanan siber di XYZ Group. Sumber data adalah wawancara dengan pihak terkait serta studi dokumenp perusahaan.
2. Studi literatur mengenai teori yang yang terkait dan akan digunakan di penelitian ini. Hasildari studi literatur ini adalah kerangka teoretis penelitian ini.
3. Pembuatan *rich pitcure* untuk menyamakan persepsi mengenai koordinasi keamanan siberdi XYZ Group.
4. Penyusunan *root definition* dengan CATWOE untuk mengidentifikasi aspek situasi dan kondisi yang perlu diubah atau transformasi.
5. Pembuatan draft *Conceptual Model* Kapabilitas *Security Operations Center* (SOC) dalam pengelolaan keamanan informasi dari analisis kondisi keamanan siber di XYZ Group dan kebutuhan keamanan informasi yang diinginkan di *Security Operations Center* (SOC) tersebut.

6. Melakukan validasi hasil *conceptual model* ke beberapa narasumber dengan wawancara dengan pihak yang terkait. Tujuannya untuk memperoleh timbal balik terhadap rancangan yang telah dibuat tersebut.
7. Melakukan identifikasi perubahan terhadap model tersebut berdasarkan timbal balik yang telah diterima.
8. Penarikan kesimpulan dan saran untuk penelitian ini.

Metode penarikan kesimpulan menggunakan penarikan kesimpulan induktif. Metode induktif adalah suatu proses yang dimulai dari observasi kejadian yang spesifik untuk kemudian ditarik ke kesimpulan yang bersifat umum (Sekaran, 2010). Dalam penelitian ini, permasalahan spesifik di ranah keamanan informasi dapat menyebabkan risiko organisasi dari segi finansial, kepatuhan regulasi, dan reputasi.

HASIL DAN PEMBAHASAN

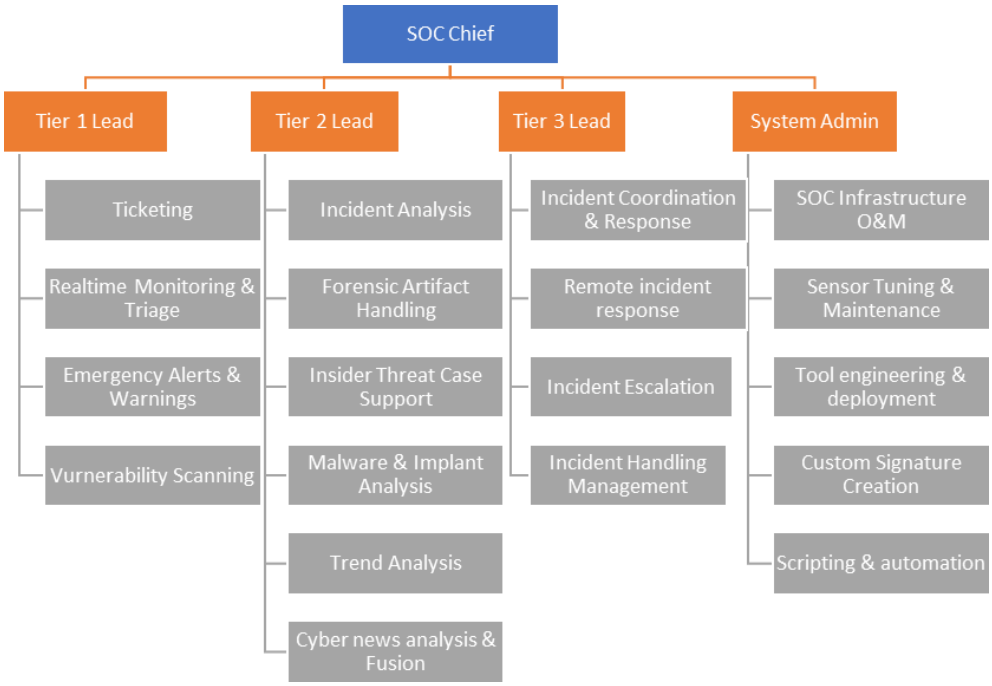
Tahap 1: Penerapan Situasi yang dianggap Problematik

a. Struktur Organisasi dan Teknologi SOC Saat Ini

Saat ini, terdapat SOC yang sedang berjalan dengan lingkup Perusahaan Induk. Diadaptasidari Zimmerman (Zimmerman, 2014), penjabaran dari jabatan yang ada di struktur tersebutmeliputi:

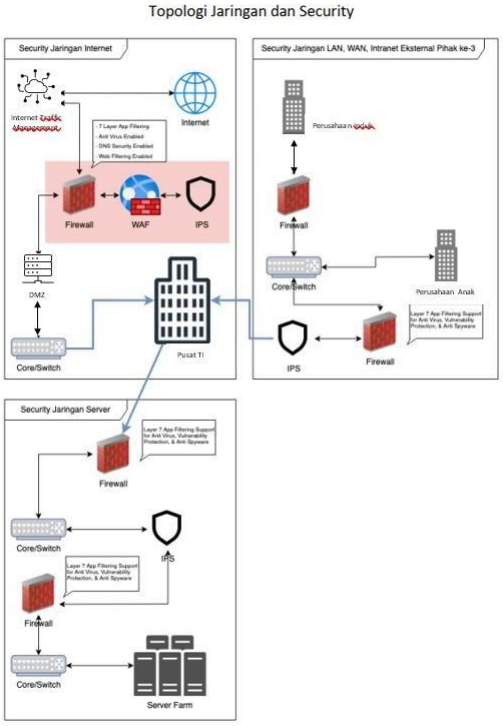
- Tier 1: Aktivitas yang lebih rutin, seperti monitoring dan analisis kejadian dan insiden keamanan siber serta mengumpulkan informasi keamanan siber, melakukan pemindaian kerentanan siber, dan menerima pengaduan atau tiket mengenai kejadian dan insiden siber.
- Tier 2: Aktivitas yang lebih mendalam dari tier 1, seperti investigasi dan korelasi suatu kejadian dan insiden siber, *incident response*, analisis log, dan pelaksanaan koordinasi respons insiden.
- Tier 3: Aktivitas yang lebih ditujukan untuk respons dan manajemen insiden siber besertaeskalasinya.
- SOC Manager / System Admin: Menjaga ketersediaan dan integritas sistem serta tools danplatform SOC dan bertanggung jawab dalam menjaga fungsionalitas SOC (update signature, scripting, maintenance) serta menerima eskalasi insiden dan pelaporan.

Penjabaran untuk setiap jabatan tersebut di organisasi tercantum di gambar 1.



Gambar 1. Struktur organisasi SOC yang berjalan di Induk Perusahaan XYZ Group

Secara keseluruhan grup perusahaan, topologi teknologi yang dipakai di Grup Perusahaandigambarkan di gambar 2.



Gambar 2. Topologi Jaringan dan Keamanan Siber di Grup Perusahaan

Seperti yang terlihat di gambar 2, beberapa teknologi keamanan sudah dipasang di jaringan tersebut. Beberapa diantaranya seperti:

- *Firewall*:perangkat yang berfungsi untuk menyaring informasi yang masuk melalui jaringan. *Firewall* dapat dikonfigurasi untuk dapat memperbolehkan atau menolak

paket data tertentu untuk masuk ke sistem.

- *Intrution Prevention* System: Suatu perangkat yang dapat menganalisis lalu lintas jaringan yang masuk atau keluar untuk mendeteksi percobaan serangan atau penyusupan kejaringan tersebut.
- *Internet Traffic Management* mengacu pada proses dan teknik yang digunakan untuk memantau, mengontrol, mengoptimalkan, dan memprioritaskan aliran lalu lintas jaringandi internet.
- *Load Balancer*: Fitur *load balancer* untuk mendistribusikan lalu lintas jaringan yang masuk di beberapa server atau sumber daya.
- *Router / Switch: Router* adalah sebuah perangkat yang berfungsi untuk melakukan koneksi antar-jaringan dan mengarahkan lalu-lintas jaringan. Sementara *switch* adalah perangkat untuk menghubungkan beberapa perangkat di suatu jaringan. *Router/switch* adalah perangkat yang menghubungkan fungsionalitas dari keduanya agar suatu paket data dapatsampai ke tujuan secara efektif.
- *Demilitarized Zone* (DMZ): Suatu area (*zone*) di suatu jaringan yang berfungsi sebagai pemisah antara jaringan internal dengan jaringan eksternal.

Untuk mendukung kebutuhan pelaksanaan SOC, beberapa teknologi yang dapat dipertimbangkan untuk ditambahkan seperti:

- *Log Platform*: Untuk mencatatat setiap kejadian dan insiden keamanan siber yang terjadi.
- Threat Hunting Analytics: Untuk menganalisa setiap kerentanan dan serangan yang terjadiatau muncul.
- *Network Detection & Response*: Mendeteksi dan merespon kejadian dan insiden siber di jaringan perusahaan.
- *Endpoint Detection Response*: Mendeteksi dan merespons kejadian dan insiden siber di perangkat *Endpoint*.
- *Security Information and Event Management* (SIEM): Mendeteksi, menganalisis, dan merespons kejadian dan ancaman siber sebelum membahayakan operasional keseluruhanoperasional bisnis.
- *User and Entity Behavior Analytics* (UEBA): Mendeteksi, menganalisis, dan merespons aktivitas pengguna / *user* agar dapat mengidentifikasi potensi titik ancaman siber.
- *Security Orchestration, Automation And Response* (SOAR): Mengkoleksikan informasimengenai kejadian dan ancaman siber untuk kemudian dapat direspons secara otomatisasi.
- *Digital Risk Protection*: Mendeteksi dan merespons ancaman digital.
- *Threat Intelligence*: Perencanaan dan pencegahan risiko digital yang terjadi.
- *Ticketing*: Menandakan suatu kejadian dan insiden siber untuk kemudian dilakukan
- *tracking*, manajemen, dan penyelesaian.

b. Analisis Wawancara

Pada tahapan ini juga telah dianalisis beberapa masalah yang muncul berdasarkan hasil wawancara yang dikategorikan berdasarkan *People, Process, dan Technology*. Berikut adalah hasilanalisis tersebut di tabel 1.

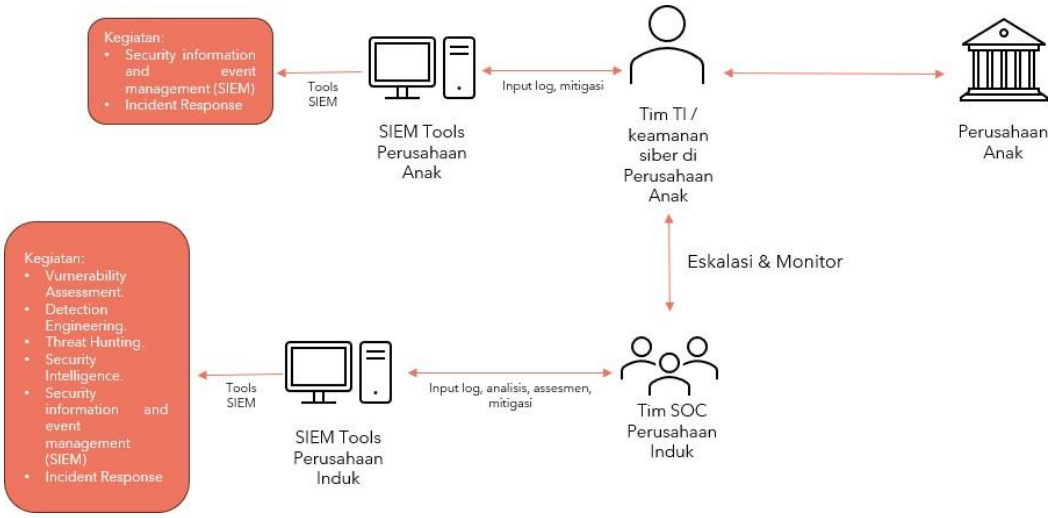
Tabel 1. Analisis Wawancara

Nomor	Transkrip	Permasalahan
1	Visibilitas mengenai status keamanan di perusahaan anak juga tidak tampak jelas di lingkup XYZ Group. Visibilitas tersebut dibutuhkan sehingga bisa diketahui komponen yang diamankan.	Proses
2	*Cybersecurity maturity* dan kesiapan di perusahaan anak dinilai masih kurang dan perlu membutuhkan suatu pengembangan kesiapan dan maturitas. Maturitas perusahaan anak tersebut belum setara dengan maturitas di perusahaan induk.	Proses & Teknologi
3	Perusahaan anak juga tidak memiliki *roadmap* untuk keamanan siber kedepannya, terlebih dalam tata kelola dan kebijakan mengenai keamanan siber.	Proses
4	Jumlah personil di perusahaan anak tidak sebanyak yang ada di induk perusahaan. Hal tersebut menyebabkan adanya rangkap jabatan di lingkup keamanan siber.	SDM
5	Dikarenakan budget yang tidak sebesar perusahaan induk, maka perusahaan anak tertinggal dalam hal teknologi. Diharapkan agar setiap anak perusahaan memiliki teknologi yang sesuai dengan kebutuhan keamanan siber mereka.	Teknologi
6	Dari segi *governance* belum ada komponen tata kelola yang tertata baik serta belum memiliki *guideline* yang terstruktur mengenai pelaksanaan operasional keamanan siber terlebih jika ada insiden.	Proses
7	Diperlukan monitoring keamanan siber di lingkup grup perusahaan yang tidak terbatas di satu perusahaan saja, seperti monitor induk ke anak dan monitor sesama perusahaan anak.	Teknologi
8	Kurangnya komunikasi antar divisi dan perusahaan menghambat penanganan insiden siber dan aktivitas keamanan siber lainnya. Harapannya adalah ketika suatu insiden di suatu perusahaan terjadi, maka bisa dikomunikasikan ke	SDM

	perusahaan lainnya sehingga mitigasi dapat diimplementasikan secara efektif dengan kerjasama di lingkup grup perusahaan serta menjadi acuan selanjutnya untuk semua perusahaan di dalam grup tersebut.	
9	Kemampuan dalam meghadapi insiden keamanan siber di beberapa perusahaan anak dirasa kurang.	SDM
10	Pengetahuan dan kesadaran mengenai keamanan siber beserta teknologinya di beberapa perusahaan anak masih belum cukup sehingga menjadi bingung ketika dihadapi suatu insiden tersebut.	SDM
11	Dibutuhkan komponen seperti Penetration Testing dimana SOC melakukan scanning terhadap aplikasi yang digunakan oleh perusahaan anak, dimana nanti kami akan melakukan menggunakan metode black box dan grey box sehingga diharapkan. Saat ini, aplikasi di perusahaan anak belum dilaksanakan Penetration Testing.	Proses
12	Dibutuhkan manajemen SOC yang terpusat yang bertanggung jawab untuk mendelegasikan atau meneruskan informasi ke divisi yang terkait apabila adanya laporan ataupun insiden yang terjadi. Informasi tersebut lebih dulu harus diketahui dan tim inilah yang akan mengkoordinasi dengan tim divisi lainnya.	Proses
13	SOC juga membutuhkan Incident Response Management yang berfungsi menentukan Standar Operasional Prosedur (SOP) untuk menghadapi suatu insiden keamanan siber. SOP ini akan dijadikan guideline untuk menghadapi respon insiden keamanan siber selanjutnya.	Proses
14	SOC juga diperlukan untuk melakukan penilaian mengenai kondisi keamanan siber perusahaan saat ini untuk keputusan strategis selanjutnya.	Teknologi
15	SOC juga diperlukan untuk melakukan Vurnerability Assesment. Kegiatan tersebut dilakukan dengan scanning terhadap aset milik perusahaan anak yang teredia atau muncul di publik sehingga bisa dilihat apakah terdapat kerentanan yang bisa ditemukan serta memberi rekomendasi perbaikan dan peningkatan.	Proses

Tahap 2: Pembuatan Rich Picture

Rich Picture yang akan dibuat akan menggambarkan situasi permasalahan terkait penyelenggaraan SOC di grup perusahaan. *Rich Pitcure* ini merupakan penjabaran dari situasi yang telah dibahas sebelumnya. Berikut adalah gambaran dari *rich picture* di gambar 3.



Gambar 3. rich picture

Berdasarkan *rich picture* di gambar 3, terdapat beberapa hal yang dapat diambil dari kondisi penyelenggaraan SOC di grup perusahaan saat ini. Diantaranya adalah:

1. SOC hanya ada di lingkup perusahaan induk. Sehingga ada kondisi dimana ketika ada kejadian atau insiden keamanan siber, maka tim TI atau keamanan siber di setiap perusahaan anak tersebut akan melapor kejadian ke perusahaan induk untuk kemudian di-*input*, dianalisis, serta proses mitigasi dengan SIEM tools yang mereka miliki.
2. Teknologi juga tidak seimbang di antara perusahaan induk dan anak. Contohnya adalah *Vurnerability Assesment* di perusahaan anak menjadi tanggung jawab utama tim SOC di perusahaan induk karena tidak adanya teknologi yang mendukung di Perusahaan Anak tersebut. Begitu pula dengan kegiatan lain seperti Incident Response Detection Engineering, Threat Hunting, dan Security Intelligence.
3. Tugas tim keamanan siber di perusahaan anak masih terbatas untuk monitoring danmencoba mitigasi insiden dan aktivitas keamanan siber yang terdeteksi.
4. Kegiatan keamanan siber akan diekspansi dengan kegiatan seperti *Penetration Testing*.

Tahap 3: Perumusan Root Definition

Perumusan root definition bertujuan untuk menampilkan gambaran yang mendalam untuk penyelenggaraaan SOC di grup perusahaan. Root Definition tersebut dirumuskan dengan menggunakan metode CATWOE untuk mengidentifikasi beberapa aspek seperti pihak yang terlibat (customer, actor, owner), kebutuhan yang diinginkan (worldview, transformasi), serta batasan atau kendala yang akan dihadapi (enviroment). Berdasarkan analisis CATWOE, maka dapat disimpulkan di tabel 2

Tabel 2. Analisis CATWOE di Grup Perusahaan

Aspek	Definisi Sistem yang terkait
Customer	Pengguna jaringan XYZ Group
Actors	Pelaku Keamanan Siber di masing-masing perusahaan (induk maupun anak) di lingkup XYZ Group.
Transformation	SOC dengan lingkup perusahaan induk → SOC dengan lingkup grup perusahaan agar keamanan seluruh anak perusahaan selaras dengan perusahaan induk.
Worldview	Dengan kapabilitas SOC ini, diharapkan setiap perusahaan di lingkup XYZ Group menjadi lebih termonitor dan terjaga untuk keamanan siber-nya.
Owner	Divisi Information Security di Perusahaan Induk.
Enviromental Constraints	Lingkup bisnis perusahaan anak yang saling berbeda sehingga tingkat teknologi juga berbeda. Budaya komunikasi antar perusahaan yang masih kurang.

Berdasarkan analisis CATWOE di tabel 2, dapat disimpulkan *root definition* yang dituju. *Root definition* tersebut adalah "Kapabilitas penyelenggaraan SOC di lingkup perusahaan induk harus dapat diperluas ke lingkup grup perusahaan sehingga seluruh perusahaan di lingkup grup perusahaan memiliki kapabilitas SOC yang sama serta memperkuat kesiapan keamanan siber".

Tahap 4 dan 5: Pembuatan Model Konseptual

a. Perbandingan Hasil Kapabilitas SOC dengan NIST *Framework*

Dalam perumusan root definition tersebut, kemudian dipetakan kapabilitas SOC dengan NIST Cybersecurity Framework. Kapabilitas SOC terdiri dari delapan fungsi dengan beberapa sub-aktivitas kemudian dihubungkan dengan kategori yang terkait di NIST framework tersebut. Pemetaan tersebut didasarkan pada kesamaan dan keterkaitan aktivitas tersebut ke dalam suatu kategori. Setiap kapabilitas SOC dapat terkait dengan satu atau lebih kategori pada NIST framework tersebut (NIST, 2014).

Hasil pemetaan Kapabilitas SOC dengan NIST Framework menunjukkan bahwa ada beberapa kapabilitas yang tidak perlu untuk perancangan kapabilitas SOC, yaitu kapabilitas Lingkungan Bisnis (ID.BE) dan Strategi Manajemen Risiko (ID.RM). Untuk lingkungan bisnis, kapabilitas tersebut tidak dimasukkan karena sub-kategori yang berkaitan dengan misi dan alur organisasi serta posisi organisasi di lingkungan bisnis dalam penyelenggaraan keamanan siber, sedangkan SOC tidak menyinggung secara langsung mengenai hal tersebut. Strategi manajemen risiko tidak dimasukkan mengingat sub-kategori yang lebih terkait dengan batas toleransi risiko, sedangkan salah satu tugas utama SOC adalah mendeteksi dan melakukan manajemen seluruh risiko tanpa melihat batas toleransi.

Dari pemetaan Kapabilitas SOC dengan NIST Framework tersebut, dapat diambil sisa kategori dari framework tersebut sebanyak 21 kategori yang terkait dengan kapabilitas SOC. Dari

21 kategori tersebut kemudian akan dianalisis kembali mengenai kapabilitas SOC yang terkait dengan sub-kategori di NIST Framework. Sub-kategori di framework tersebut dapat memiliki satu atau lebih kapabilitas SOC. Hasil analisis yang diharapkan adalah sub-kategori beserta kapabilitas SOC yang terkait untuk penyelenggaraan SOC yang efektif. 31

Dari hasil analisis ini, ditemukan sebanyak 90 aktivitas yang tersebar di 21 kategori. Setelah itu adalah analisis gap dari aktivitas tersebut dengan kondisi sebenarnya yang telah terdeteksi di tahapan sebelumnya yang utamanya berdasarkan hasil wawancara, studi dokumen, dan observasi langsung SOC di perusahaan induk.

Hasil dari analisis tersebut adalah bahwa dari 90 aktivitas tersebut, sebanyak 31 aktivitas masih belum dilaksanakan atau belum optimal dalam pelaksanaannya. Aktivitas tersebut dapat menjadi perhatian bagi operasional keamanan siber di grup perusahaan untuk mengembangkan lingkup SOC dari lingkup perusahaan induk menjadi lingkup grup perusahaan. Hasil tersebut kemudian dianalisis kembali menggunakan Model RACI serta akan ditetapkan prioritasi aktivitas berdasarkan urgensi dan dampak.

Berikut dijabarkan aktivitas yang perlu ditingkatkan agar SOC dengan lingkup yang lebih luas dapat meningkatkan kapabilitas mereka secara efektif di tabel 3 berikut.

Tabel 3. Pemetaan Kapabilitas SOC yang Perlu Ditingkatkan di Grup Perusahaan dengan NIST *Framework*

Fungsi Kerja				**Kapabilitas SOC**	**Aktivitas**
ID	**Nama**	**ID.Kat**	**Kategori**		
ID	***Identify***	***ID.AM***	***Asset Management***	• *Training & Awareness Building* • *Situational Awareness*	***ID.AM-3:*** *Organizational communication and data flows are mapped*
				• Konsultasi Keamanan	***ID.AM-5:*** *Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value*

					ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
		ID.GV	***Governance***	• *Security Consulting* • Dukungan Ancaman dari Internal Organisasi • *Redistribution of TTPs*	***ID.GV-3:*** *Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.*
		ID.RA	***Risk Assessment***	• Penilaian Ancaman • Analisis Tren & Historis • Analisis Insiden • Riset & Kajian Insiden • *Penetrati on Testing*	***ID.RA-2:*** *Cyber threat intelligence is received from Information sharing forumsand sources.* *ID.RA-4: Potential business impacts and likelihoods are identified.*
PR	***Protect***	***PR.AT***	***Awareness & Training***	• *Training & Awareness Building*	***PR.AT-1:*** *All users are informed and trained.*

		• *Situational Awareness*	***PR.AT-5:*** *Physical and cybersecurity personnel understand their roles and responsibilities.*
PR.DS	***Data Security***	Perangkat Proteksi Area *Demilitarized Zone* (DMZ)	***PR.DS-5:*** *Protections against data leaks are implemented.*
PR.IP	***Information Protection Process & Procedures***	• Implementasi Penanganan • *Redistribution of TTPs* • Eskalasi dan Koordinasi Penanganan Insiden	***PR.IP-5:*** *Policy and regulations regarding the physical operating environment for organizational assets are met* ***PR.IP-7:*** *Protection processes are improved.* ***PR.IP-8:*** *Effectiveness of protection technologies is shared* *PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster*

			Recovery) are in place and managed *PR.IP-10: Response and recovery plans are tested* *PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)* *PR.IP-12: A vulnerability management plan is developed and implemented*
PR.PT	***Protective Technology***	• Infrastruktur Pendukung SOC • Penanganan Artifak untuk Kepentingan Forensik • Perangkat Proteksi Area Demilitarized Zone (DMZ)	***PR.PT-5:*** *Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations*

DE	***Detect***	***DE.CM***	***Security Continuous Monitoring***	• Situational Awareness • Pemindaian Kerentanan	***DE.CM-7:*** *Monitoring for unauthorized personnel, connections, devices, and software is performed* ***DE.CM-8:*** *Vulnerability scans are performed*
		DE.DP	***Detection Processes***	• Pemindaian Kerentanan • Koleksi dan Distribusi Data Audit	***DE.DP-1:*** *Roles and responsibilities for detection are well defined to ensure accountability* ***DE.DP-3:*** *Detection processes are tested* ***DE.DP-4:*** *Event detection information is communicated* ***DE.DP-5:*** *Detection processes are continuously improved*
RS	***Respond***	***RS.RP***	***Response Planning***	• *Redistribution of TTPs* • Penilaian Ancaman • Penanganan Insiden	***RS.RP-1:*** *Response plan is executed during or after an incident*

		RS.CO	***Communi-cations***	• *Redistribution of TTPs* • Eskalasi dan Koordinasi Penanganan Insiden	***RS.CO-1:*** *Personnel know their roles and order of operations when a response is needed* ***RS.CO-2:*** *Incidents are reported consistent with established criteria* ***RS.CO-3:*** *Information is shared consistent with response plans* ***RS.CO-4:*** *Coordination with stakeholders occurs consistent with response plans*
RC	***Recover***	***RC.RP***	***Recover Planning***	• Product Assessment • Penilaian Kerentanan • Penanganan Artifak untuk Kepentingan Forensik • Penagnanan Insiden Melalui Remote • Penagnanan Insiden di lapangan • Penilaiajn Ancaman	***RC.RP-1:*** *Recovery plan is executed during or after a cybersecurity incident*

- Pemantauan *Real-time*
- *Redistribution of TTPs*
- Eskalasi dan Koordinasi Penanganan Insiden

b. Pemetaan Aktivitas di NIST Cybersecurity Framework dengan Matriks RACI

Selanjutnya, NIST Cybersecurity Framework yang perlu ditingkatkan tersebut kemudian ditetapkan mengenai siapa yang akan melakukan suatu tugas, yang bertanggung jawab, yang dapat dikonsultasikan, dan yang mendapat informasi. Pemetaan tersebut akan menggunakan Matriks RACI. Penjelasan dari Matriks RACI tercantum dalam tabel 4 berikut (Institute, 2021).

Tabel 4. Penjelasan Matriks RACI

Aspek	Deksripsi
***Responsible* (R)**	Yang melakukan pekerjaan tersebut.
***Accountable* (A)**	Yang bertanggung jawab atas penyelesaian tugas tersebut.
***Consulted* (C)**	Yang diambil pendapat dan masukan dari mereka.
***Informed* (I)**	Yang cukup terinfokan dan *up-to-date.*

Setelah NIST Cybersecurity Framework tersebut disesuaikan dengan role jabatan dan dikonsultasikan dengan dikonsultasikan dengan subject matter expert (SME), maka hasil dari pemetaan kegiatan NIST Cybersecurity Framework dengan Matriks RACI didapatkan di tabel 5 berikut.

Tabel 5. Pemetaan Aktivitas di NIST *Framework* dengan Matriks RACI

Sub-Aktivitas	SOC Chief	SOC Manager	Tier 1	Tier 2	Tier 3	SystemLead
ID.AM-3: *Organizational communication and data flowsare mapped*	A	R	I	I	I	C
ID.AM-5: *Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value*	R	A	I	I	I	C
ID.AM-6: *Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established*	A	R	I	I	I	C
ID.GV-3: *Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed*	R	A	I	I	I	C
ID.RA-2: *Cyber threat intelligence is received from information sharing forums andsources*	A	C	I	I	I	R
ID.RA-4: *Potential business impacts and likelihoods are identified*	C	A	I	I	I	R
PR.AT-1: *All users are informed and trained*	A	R	C	C	C	C
PR.AT-5*: Physical and cybersecurity personnel*	A	R	I	I	I	I

understand their roles and responsibilities						
PR.DS-5: *Protections against data leaks are implemented*	I	A	A	-	-	R
PR.IP-5: *Policy and regulations regarding the physical operating environment for organizational assets are met*	A	R	I	I	I	C
PR.IP-7: *Protection processes are improved*	I	A	R	-	-	C
PR.IP-8: *Effectiveness of protection technologies is shared*	A	C	I	I	I	R
PR.IP-9: *Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed*	C	A	I	I	R	I
PR.IP-10: *Response and recovery plans are tested*	I	C	A	A	R	I
DE.DP-4*: Event detection information is communicated*	I	A	C	C	R	C
DE.DP-5: *Detection processes are continuously improved*	I	A	R	C	C	C
RS.RP-1: *Response plan is executed during or after an incident*	I	R	C	C	R	C
RS.CO-1: *Personnel know their roles and order of operations when a response is needed*	I	A	R	-	-	C
RS.CO-2: *Incidents are reported consistent with established criteria*	A	C	I	I	I	R
RS.CO-3: *Information is shared consistent with response plans*	C	A	I	I	R	I
RS.CO-4: *Coordination with stakeholders occurs consistent*	I	C	A	A	R	I

with response plans						
PR.IP-11: *Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)*	-	A	A	-	-	R
PR.IP-12: *A vulnerability management plan is developed and implemented*	-	A	R	I	I	C
PR.PT-5: *Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations*	I	A	-	-	-	R
DE.CM-7: *Monitoring for unauthorized personnel, connections, devices, and software is performed*	A	I	R	-	-	C
DE.CM-8: *Vulnerability scans are performed*	A	I	R	-	-	C
DE.DP-1: *Roles and responsibilities for detection are well defined to ensure accountability*	A	R	I	I	I	I
DE.DP-3: *Detection processes are tested*	I	A	R	-	-	C
DE.DP-4: Event detection information is *communicated*	I	A	C	I	R	I
DE.DP-5: *Detection processes are continuously improved*	I	A	R	-	-	C
RS.RP-1: *Response plan is executed during or after an incident*	I	A	C	C	R	C
RS.CO-1: *Personnel know their roles and order of operations when a response is needed*	C	R	I	I	I	I
RS.CO-2: *Incidents are reported consistent with established criteria*	C	C	I	I	I	R

RS.CO-3: *Information is shared consistent with response plans*	C	A	I	I	R	I
RS.CO-4: *Coordination with stakeholders occurs consistent with response plans*	I	C	A	A	R	I
RC.RP-1: *Recovery plan is executed during or after a cybersecurity incident*	A	R	C	C	C	C
RC.CO-3: *Recovery activities are communicated to internal and external stakeholders as well as executive and management Teams*	A	R	C	C	C	C

a. Pemetaan Aktivitas di NIST Cybersecurity Framework dengan Matriks RACI

Setelah pemetaan terhadap matriks RACI ke setiap jabatan SOC, kemudian setiap aktivitasNIST *Cybersecurity Framework* tersebut dipetakan berdasarkan dampak dan urgensi dari setiap kegiatan. Dampak didefinisikan sebagai pihak siapa yang akan terkena konsekuensi atau dampak dikarenakan suatu kegiatan tertentu. Sedangkan urgensi didfinisikan sebagai kepentingan atau urgensi terhadap waktu pelaksanaan kegiatan tertentu agar tujuan dari suatu aktivitas tersebut tercapai.

Lingkup dari dampak didefinisikan di tabel 6. Sedangkan gambaran waktu berdasarkan urgensi didefinisikan di tabel 7.

Tabel 6. Tabel Dampak

Dampak	Arti
Dampak 1	Berdampak terhadap *Hardware/ Software*
Dampak 2	Berdampak terhadap SOC Internal
Dampak 3	Berdampak terhadap instansi / grup
Dampak 4	Berdampak kepada pihak eksternal / stakeholder
Dampak 5	Berdampak nasional dan dunia

Tabel 7. Tabel Urgensi

Urgensi	Arti
Urgensi 1	Tidak segera
Urgensi 2	Fleksibel / pendukung
Urgensi 3	Segera untuk dilakukan
Urgensi 4	Sangat segera untuk dilakukan
Urgensi 5	Bersifat langsung (*real time*) dan sangat segera untuk dilakukan

Hubungan antara urgensi dan dampak membentuk suatu prioritas. Prioritas mendefinisikan suatu aktivitas yang perlu diperhatikan dan dijalankan terlebih dahulu agar proseskapabilitas SOC berjalan secara efektif. Hubungan keduanya tersebut digambarkan dalam tabel 8.

Tabel 8. Tabel Prioritas

Prioritas	Urgensi 5	Urgensi 4	Urgensi 3	Urgensi 2	Urgensi 1
Dampak 5	Prioritas 5	Prioritas 5	Prioritas 5	Prioritas 4	Prioritas 3
Dampak 4	Prioritas 5	Prioritas 4	Prioritas 4	Prioritas 3	Prioritas 2
Dampak 3	Prioritas 5	Prioritas 4	Prioritas 3	Prioritas 2	Prioritas 1
Dampak 2	Prioritas 4	Prioritas 3	Prioritas 2	Prioritas 2	Prioritas 1
Dampak 1	Prioritas 3	Prioritas 2	Prioritas 1	Prioritas 1	Prioritas 1

Untuk *Person In Contact* masing-masing aktivitas, ditetapkan berdasarkan matriks RACI dimana jabatan tersebut memegang tanggung jawab masing-masing. Berdasarkan pendefinisian dampak, urgensi, dan prioritas tersebut serta setelah konsultasi dengan *subject matter expert*, makaprioritas dari beberapa sub-ktivitas di NIST *Cybersecurity Network* serta PIC digambarkan di tabel9 berikut.

Tabel 9. Tabel Prioritas Sub-Aktivitas Beserta PIC

Sub-Aktivitas	Dampak	Urgensi	Prioritas	PIC
ID.AM-3: Organizational communication and dataflows are mapped	4	2	4	SOC Manager
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	3	2	4	SOC Chief
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g.,suppliers, customers, partners) are established	4	3	4	SOC Manager
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civilliberties obligations, are understood and managed	3	3	3	SOC Chief
ID.RA-2: Cyber threat intelligence is received frominformation sharing forums and sources	2	1	1	System Lead
ID.RA-4: Potential businessimpacts and likelihoods are identified	4	3	4	System Lead

PR.AT-1: All users are informed and trained	3	4	4	SOC Manager
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	3	3	3	SOC Manager
PR.DS-5: Protections against data leaks are implemented	4	4	4	System Lead
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	3	2	2	SOC Manager
PR.IP-7: Protection processes are improved	3	4	4	Tier 1
PR.IP-8: Effectiveness of protection technologies is shared	2	2	2	System Lead
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	5	5	4	Tier 3
PR.IP-10: Response and recovery plans are tested	3	4	4	Tier 3
DE.DP-4: Event detection information is communicated	5	5	5	Tier 3
DE.DP-5: Detection processes are continuously improved	4	4	4	Tier 1
RS.RP-1: Response plan is executed during or after an incident	5	5	5	Tier 3
RS.CO-1: Personnel know their roles and order of operations when a response is needed	3	4	4	Tier 1
RS.CO-2: Incidents are reported consistent with established criteria	3	2	3	System Lead

RS.CO-3: Information is shared consistent with response plans	4	3	4	Tier 3
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	4	3	4	Tier 3
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	3	4	4	System Lead
PR.IP-12: A vulnerability management plan is developed and implemented	5	5	5	Tier 1
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	3	5	5	System Lead
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	5	5	5	Tier 1
DE.CM-8: Vulnerability scans are performed	3	5	5	Tier 1
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	3	4	4	SOC Manager
DE.DP-3: Detection processes are tested	3	4	4	Tier 1
DE.DP-4: Event detection information is communicated	4	5	5	Tier 3
DE.DP-5: Detection processes are continuously improved	3	4	4	Tier 1
RS.RP-1: Response plan is executed during or after an incident	5	5	5	Tier 3
RS.CO-1: Personnel know their roles and order of operations when a response	3	4	4	SOC Manager

is needed				
RS.CO-2: Incidents are reported consistent with established criteria	5	4	5	System Lead
RS.CO-3: Information is shared consistent with response plans	3	3	3	Tier 3
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	4	3	4	Tier 3
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	5	5	5	SOC Manager
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	4	4	4	SOC Manager

Dari tabel 9 tersebut, terlihat bahwa dari 31 aktivitas yang perlu diperhatikan, ada 8 aktivitas dengan prioritas tertinggi atau dengan skor prioritas 5. Aktivitas tersebut diantaranya adalah:

- DE.DP-4: Informasi deteksi kejadian dikomunikasikan.
- RS.RP-1: Rencana respons dilaksanakan selama atau setelah insiden.
- PR.IP-12: Rencana manajemen kerentanan dikembangkan dan diimplementasikan.
- PR.PT-5: Mekanisme (*failsafe, load balancing, hot swap*) diterapkan untuk mencapaipersyaratan ketahanan dalam situasi normal dan buruk.
- DE.CM-7: Pemantauan terhadap personil, koneksi, perangkat, dan perangkat lunak yangtidak sah dilakukan.
- DE.CM-8: Pemindaian kerentanan dilakukan.
- RS.CO-2: Insiden dilaporkan sesuai dengan kriteria yang telah ditetapkan.
- RC.RP-1: Rencana pemulihan dilaksanakan selama atau setelah insiden keamanan siber.

SIMPULAN

Penelitian ini bertujuan untuk memberikan usulan untuk rancangan kapabilitas SOC kepada PT XYZ sehingga dapat membantu mengatasi permasalahan keamanan siber di lingkup grup perusahaan. Penelitian ini juga menyorot beberapa kapabilitas SOC yang perlu peningkatan. Dari penelitian ini, didapat bahwa dari sebanyak 90 sub-aktivitas di NIST Framework, sebanyak 31 sub-aktivitas perlu diperhatikan untuk pengembangan SOC. Dari 31 sub-aktivitas tersebut, didapat aktivitas dengan prioritas yang paling tinggi (dengan skor 5) sejumlah 8 sub-aktivitas, yang dapat

diartikan sebagai aktivitas yang paling diutamakan untuk dilaksanakan atau ditingkatkan. Diharapkan dengan adanya hasil penelitian ini, penyelenggaraan SOC di lingkup grup perusahaan dapat berjalan lebih efektif.

BIBLIOGRAFI

Asosiasi Penyelenggara Jasa Internet Indonesia (2020, 20 Desember). Laporan Survei Internet APJII 2019 - 2020 [Q2]. Diambil dari https://apjii.or.id/survei2019x/download/4anJWTMIQgtzjV95UD0sPYXC6xGk8v

Cyber Magazine. (2021, October 26). Top 10 cyber security threats. https://cybermagazine.com/cyber-security/top-10-cyber-security-threats

Institute, P. M. (2021). A Guide to the Project Management Body of Knowledge (Pmbok(r) Guide) - Seventh Edition. Pmbok(r) Guide.

Jackson, M. C. (2003). SYSTEMS THINKING: Creative Holism for Managers. International Journal of General Systems (Vol. 35). John Wiley and Sons. https://doi.org/10.1002/sres

Mansfield-Devine, S. (2022). IBM: Cost of a Data Breach. Network Security, 2022(8). https://doi.org/10.12968/s1353-4858(22)70049-9

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 1–41. https://doi.org/10.1109/JPROC.2011.2165269

Otoritas Jasa Keuangan (2016). Peraturan OJK No.38/POJK.3/2016 Tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Oleh Bank Umum

Otoritas Jasa Keuangan (2022). Peraturan OJK No.11/POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.

Sekaran, U dan Bougie (2010). Research Methods for Business: A Skill-Building Approach, John Wiley and sons inc: London

Zimmerman, C. (2014). Cybersecurity Operations Center. Retrieved from https://www.web3us.com/sites/default/files/mitre-10-strategies-cyber-ops-center.pdf