The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 4, August 2025
https://doi.org/10.33022/ijcs.v14i4.4945

Perancangan Kapabilitas Security Operations Center di Public Cloud Computing Environment: Studi Kasus PT. XYZ

M Ryan Fadholi[1], Rizal Fathoni Aji[2]
m.ryan11@ui.ac.id[1], rizal@cs.ui.ac.id[2]
[1,2]Faculty of Computer Science, Universitas Indonesia, Jakarta, Indonesia

Informasi Artikel

Diterima : 5 Jul 2025
Direvisi : 21 Jul 2025
Disetujui : 3 Agu 2025

Kata Kunci

information security, security operations center, cloud computing, SOC-CMM, NIST Cybersecurity Framework

Abstrak

Keamanan siber saat ini telah menjadi tantangan utama bagi institusi keuangan, termasuk bagi PT. XYZ. PT. XYZ saat ini telah memiliki *Security Operations Center* (SOC) untuk pengamanan siber perusahaan, namun tim SOC tersebut belum memiliki kapabilitas yang optimal dalam memantau lingkungan public cloud yang saat ini mulai diadopsi perusahaan. Hal ini menyebabkan adanya risiko serangan siber yang tidak terdeteksi pada *public cloud* perusahaan. Penelitian ini bertujuan menyusun rekomendasi pengembangan kapabilitas SOC di lingkungan *public cloud* PT. XYZ menggunakan metodologi *Design Science Research* (DSRM). Analisis kondisi awal tim SOC dilakukan berdasarkan observasi dan analisis dokumen. Kemudian, dilakukan identifikasi *gap* dilakukan melalui FGD berdasarkan pertanyaan pada SOC-CMM *screening* tool. NIST *Cybersecurity Framework* (CSF) kemudian digunakan sebagai framework dalam menyusun kapabilitas yang diharapkan. Hasil dari penelitian ini adalah sebuah rancangan rekomendasi peningkatan kapabilitas tim SOC berupa 35 rekomendasi praktis bagi PT. XYZ yang dikategorikan sesuai domain SOC-CMM.

Keywords

information security, security operations center, cloud computing, SOC-CMM, NIST Cybersecurity Framework

Abstract

Cybersecurity has become a major challenge for financial institutions, including PT. XYZ. Although PT. XYZ has established a Security Operations Center (SOC) to safeguard its digital assets, the current SOC team lacks optimal capability to monitor the organization's newly adopted public cloud environment. This gap increases the risk of undetected cyberattacks targeting the cloud infrastructure. This study aims to develop recommendations for enhancing SOC capabilities in PT. XYZ's public cloud environment using the Design Science Research (DSR) method. The initial SOC condition was analyzed through document review and observation. Capability gaps were identified through focus group discussions (FGD) guided by the SOC-CMM screening tool. The NIST Cybersecurity Framework (CSF) was then employed as the foundation for defining target capabilities. The study resulted in a set of 35 practical recommendations to improve the SOC team's capabilities, categorized according to the SOC-CMM domains.

A. Pendahuluan

Keamanan siber merupakan aspek krusial dalam industri jasa keuangan, terutama bagi institusi perbankan yang memiliki kewajiban untuk menjaga ketahanan sistem informasi. Sesuai dengan peraturan Otoritas Jasa Keuangan (OJK) Indonesia, bank umum diwajibkan untuk menjaga ketahanan siber dan memastikan proses keamanan tersebut didukung dengan sistem yang memadai [1]. Kegagalan dalam menjaga keamanan siber dapat mengakibatkan insiden yang bersifat eksistensial, termasuk kerugian finansial yang signifikan [2] dan turunnya kepercayaan nasabah [3]. PT. XYZ sebagai salah satu institusi perbankan terbesar di Indonesia telah merespons tantangan ini dengan membangun sistem pengamanan siber menyeluruh, termasuk dengan pembangunan *Security Operations Center* (SOC). SOC bertugas melakukan pemantauan, pencegahan, dan penanganan insiden keamanan informasi guna menjaga *situational awareness* serta memenuhi tuntutan regulasi [4].

Security Operations Center (SOC) merupakan sebuah fungsi dalam organisasi yang berperan sebagai pusat pemantauan dan pengelolaan keamanan informasi yang terintegrasi. SOC mengombinasikan unsur manusia (*people*), proses (*process*), dan teknologi (*technology*), untuk meningkatkan postur keamanan siber secara menyeluruh dalam organisasi. Kegiatan utama dari tim SOC adalah mendeteksi ancaman sedini mungkin dan mengkoordinasikan respons yang efektif sebelum ancaman tersebut menimbulkan kerugian [4].

Namun, meningkatnya kompleksitas lingkungan teknologi informasi (TI), khususnya akibat adopsi *cloud computing*, telah menimbulkan tantangan baru bagi SOC. Sesuai perkembangan teknologi dan kebutuhan bisnis, PT. XYZ telah mengadopsi *cloud computing* melalui penggunaan *public cloud* di perusahaan. *Cloud computing* merupakan model penyediaan infrastruktur dimana sumber daya *computing* (*server*, jaringan, *storage*, dll) dapat disediakan secara cepat dari sebuah *shared pool* dengan kebutuhan manajemen dan interaksi dengan penyedia jasa yang minimal [5]. Salah satu model layanan *cloud computing* yang populer digunakan adalah *public cloud*, dimana sumber daya komputasi disediakan oleh pihak ketiga dan digunakan melalui internet oleh pengguna.

Meskipun menawarkan efisiensi, *public cloud* juga membawa risiko keamanan seperti kebocoran data dan akses tidak sah [6]. Sayangnya, tim SOC PT. XYZ belum memiliki kapabilitas yang memadai untuk memantau keamanan di lingkungan *public cloud* tersebut, yang menyebabkan timbulnya risiko serangan siber pada aplikasi berbasis *cloud* milik PT. XYZ. Hal ini merupakan gap kapabilitas dalam pengamanan *cloud environment* perusahaan. Berdasarkan kondisi tersebut, dibutuhkan rancangan pengembangan kapabilitas tim SOC yang mampu menjawab kebutuhan pengamanan lingkungan *cloud* PT. XYZ.

B. Metode Penelitian

Penelitian ini menggunakan **Design Science Research Methodology (DSRM)**. DSRM adalah pendekatan kualitatif berbasis desain yang bertujuan menciptakan *artifact* (dalam hal ini rekomendasi pengembangan kapabilitas) untuk memecahkan permasalahan nyata yang terjadi pada organisasi. Metode ini banyak digunakan dalam riset sistem informasi karena mampu menggabungkan kontribusi praktis dan akademik, atas *artifact* yang dikembangkan [7].

Dalam penelitian ini, DSRM digunakan untuk merancang kapabilitas *Security Operations Center* (SOC) yang mampu memantau lingkungan *public cloud computing* di PT. XYZ. Penyesuaian tahapan dilakukan berdasarkan konteks organisasi yang menekankan pentingnya proses iteratif dalam pengembangan SOC [8]. Tahapan dari penelitian ini dengan pendekatan DSRM adalah sebagai berikut:

I. Identifikasi Kebutuhan

Pada tahap ini dilakukan *document review* dan *focus group discussion* bersama beberapa *expert* dalam tim SOC PT. XYZ kuesioner SOC-CMM *screening tool* untuk mengetahui ekspektasi *stakeholder*, kondisi tim SOC saat ini, serta gap antara kondisi saat ini dan ekspektasi *stakeholder*. Metode FGD dipilih sesuai rekomendasi tim SOC-CMM untuk melakukan assessment dalam bentuk diskusi dengan beberapa expert dengan role yang berbeda dalam SOC untuk memfasilitasi diskusi [9].

Document review dilakukan untuk memperoleh data sekunder yang digunakan dalam menjalankan penelitian. Dokumen yang dianalisis dalam penelitian ini terdiri dari penelitian sebelumnya dan dokumen internal perusahaan.

Selanjutnya FGD dilakukan untuk mengetahui kondisi kapabilitas tim SOC PT. XYZ saat ini dalam melakukan pengamanan dan pemantauan *public cloud environment*. Pertama-tama, dilakukan pemilihan narasumber untuk FGD dilakukan dengan mempertimbangkan *role* dan keahlian masing-masing narasumber, sehingga *expertise* narasumber yang berpartisipasi mencakup keseluruhan kegiatan tim SOC. Tabel 1 menjabarkan narasumber yang berpartisipasi:

Tabel 1. Daftar Peserta Focus Group Discussion

No	Narasumber	Keahlian	Pengalaman	Alasan Pemilihan
1	Te*am Member Cyber Intelligence & Analysis Center*	*SOC Governanc*e	6 tahun di *Cybersecurity/* ISO270001 lead implementor	Berpengalaman sebagai *person-in-charge* dalam kegiatan audit tim SOC PT. XYZ baik internal maupun eksternal
2	SOC Manager	*SOC Governance, SOC Operations*	21 tahun di *Cybersecurity/* CISSP	Bertanggung jawab terhadap operasional *monitoring* tim SOC PT. XYZ, dengan pengalaman menyusun kapabilitas tim SOC di berbagai organisasi
3	Threat Hunting Lead	*SOC Operations*	10 tahun di *Cybersecurity/* GIAC Continuous Monitoring	Bertanggung jawab terhadap operasional *threat hunting* & *detection engineering* tim SOC PT. XYZ, dengan pengalaman sebagai konsultan peningkatan kapabilitas SOC di berbagai organisasi

Selanjutnya struktur pembahasan pada FGD disusun berdasarkan pertanyaan yang disadur dari SOC-CMM *screening tool* untuk memfasilitasi diskusi. SOC-CMM *screening tool* merupakan asesmen berbasis framework SOC-CMM dengan metode kuisioner atau *self-assessment* yang bersifat *high-level* dam dapat memberikan gambaran umum mengenai kapabilitas umum sebuah SOC [9].

SOC-CMM (Security Operations Center Capability Maturity Model) merupakan sebuah kerangka kerja yang dikembangkan untuk membantu organisasi dalam menilai dan meningkatkan tingkat kematangan kapabilitas *Security Operations Center* (SOC) yang dimilikinya. *Framework* ini dirancang sebagai alat bantu evaluasi

menyeluruh yang mencakup berbagai aspek penting dalam operasional SOC, dengan pendekatan berbasis dimensi dan indikator kapabilitas [10]. Penilaian kapabilitas dalam SOC-CMM dilakukan berdasarkan lima *domain* utama yang mewakili elemen-elemen fundamental dalam pengelolaan SOC yaitu:

1. ***Business*****:** Menilai sejauh mana peran dan fungsi SOC terintegrasi dengan strategi dan objektif bisnis organisasi. Dimensi ini mencakup pengukuran terhadap nilai tambah SOC terhadap keberlangsungan operasional organisasi secara keseluruhan.
2. ***People*****:** Menilai aspek sumber daya manusia dalam SOC, termasuk struktur tim, kapasitas, kompetensi teknis, dan jalur pengembangan profesional bagi personel SOC.
3. ***Process*****:** Menganalisis keberadaan dan kematangan proses yang diterapkan dalam operasional SOC, termasuk dokumentasi, penerapan, serta konsistensi eksekusi dari proses-proses keamanan yang ada.
4. ***Technology*****:** Menilai infrastruktur teknologi dan alat bantu yang digunakan untuk mendukung aktivitas pemantauan, deteksi, respons, dan pelaporan insiden keamanan siber.
5. ***Services*****:** Meninjau cakupan layanan yang disediakan oleh SOC, baik layanan reaktif seperti *incident response* maupun layanan proaktif seperti *threat hunting* dan *threat intelligence*, serta bagaimana layanan tersebut diintegrasikan dengan kebutuhan pengguna internal.

Pembahasan dalam FGD tersebut terbagi menjadi 5 domain sebagai berikut:

1. Domain *Business*

Tabel 2. Daftar Pertanyaan FGD (Domain *Business*)

Subkategori	Kode	Pertanyaan
Business Drivers	B.1.1	*Business drivers* telah diidentifikasi
	B.1.2	*Business drivers* telah didokumentasikan
	B.1.3	*Business drivers* telah diverifikasi dan disetujui
	B.1.4	*Business drivers* diperbarui secara berkala
	B.1.5	*Business drivers* digunakan secara aktif dalam pengambilan keputusan
Customers	B.2.1	*Customer/stakeholder* telah diidentifikasi
	B.2.2	Customer/stakeholdertelah didokumentasikan
	B.2.3	Kebutuhan informasi Customer/stakeholder kepentingan telah dipahami
	B.2.4	Informasi pelanggan/pemangku kepentingan diperbarui secara berkala
	B.2.5	Kepuasan *customer/stakeholder* diukur dan ditingkatkan
Charter	B.3.1	Elemen *SOC charter* telah diidentifikasi
	B.3.2	*SOC charter* telah didokumentasikan
	B.3.3	Isi *SOC charter* telah diverifikasi dan disetujui
	B.3.4	*SOC charter* diperbarui secara berkala
	B.3.5	*SOC charter* telah digunakan untuk memberikan informasi kepada *customer/stakeholder*
Governance	B.4.1	Elemen tata kelola telah diidentifikasi
	B.4.2	Proses tata kelola telah didokumentasikan

	B.4.3	Proses tata kelola SOC telah dioperasionalkan melalui *meeting* yang melibatkan pihak-pihak terkait
	B.4.4	Proses tata kelola SOC dievaluasi secara berkala
	B.4.5	Efektivitas proses tata kelola SOC diukur dan ditingkatkan
	B.5.1	Kebijakan keamanan yang mendukung SOC telah tersedia
	B.5.2	Kebijakan SOC yang menjelaskan cara kerja SOC telah tersedia
	B.5.3	Kebijakan SOC diperbarui secara berkala
Privacy & Policy	B.5.4	Persyaratan privasi dipahami dan diintegrasikan dalam prosedur SOC
	B.5.5	*Privacy impact analysis* dilaksanakan dan hasilnya digunakan untuk perbaikan

2. Domain *People*

Tabel 3. Daftar Pertanyaan FGD (Domain *People*)

Subkategori	Kode	Pertanyaan
	P.1.1	Tingkat kebutuhan personel SOC telah diketahui
	P.1.2	Kebutuhan karyawan tetap (jumlah personel) telah dipenuhi
Employees	P.1.3	Proses akuisisi dan pengembangan talenta telah diterapkan dan berjalan efektif
	P.1.4	Strategi *sourcing* dan *retainment* telah tersedia dan efektif
	P.1.5	SOC menyedian lingkungan psikologis yang aman
	P.2.1	Struktur tim SOC dioptimalkan sesuai ukuran dan strukturnya
	P.2.2	Hierarki SOC (termasuk sistem *tiering* jika berlaku) telah diterapkan dan berfungsi efektif
Roles & Hierarchy	P.2.3	Deskripsi peran SOC telah didokumentasikan, disetujui, dan diperbarui secara berkala
	P.2.4	Deskripsi peran dipahami oleh karyawan SOC
	P.2.5	Deskripsi peran digunakan dalam proses rekrutmen dan pengembangan karir
	P.3.1	Jalur pengembangan karir telah ditetapkan
	P.3.2	Sasaran individu dan tim telah didefinisikan dan dimonitor
People Management	P.3.3	Karyawan baru disaring dan di-*onboard* ke SOC dengan proses yang terstandarisasi
	P.3.4	Karyawan SOC dievaluasi dan dibimbing untuk mendukung pengembangan mereka
	P.3.5	Kepuasan karyawan diukur dan hasilnya digunakan untuk perbaikan
	P.4.1	Proses manajemen pengetahuan telah didokumentasikan, diterapkan, dan berjalan efektif
	P.4.2	Proses manajemen pengetahuan telah disetujui dan ditinjau secara berkala
Knowledge Management	P.4.3	Manajemen pengetahuan didukung secara efektif oleh perangkat pendukung
	P.4.4	*Knowledge* dan *skill matrix* telah disusun dan dipelihara
	P.4.5	*Knowledge* dan *skill matrix* digunakan secara aktif untuk mengatasi *single points of knowledge/skill*
	P.5.1	Program pelatihan telah diterapkan dan berjalan efektif
	P.5.2	Program sertifikasi telah diterapkan dan berjalan efektif
Training & Education	P.5.3	Pelatihan dan sertifikasiyang bersifat wajib telah dimonitor untuk setiap karyawan SOC
	P.5.4	Sumber daya (anggaran & waktu) untuk pelatihan, pendidikan, dan sertifikasi telah dialokasikan
	P.5.5	*Workshop* dan kegiatan lainnya untuk pengembangan pengetahuan telah diadakan secara berkala

3. Domain *Process*

Tabel 4. Daftar Pertanyaan FGD (Domain *Process*)

Subkategori	Kode	Pertanyaan
SOC Management	M.1.1	Elemen manajemen SOC telah diidentifikasi
	M.1.2	Proses manajemen SOC telah didokumentasikan, diterapkan, dan berjalan efektif
	M.1.3	Proses manajemen SOC diperbarui dan ditingkatkan secara berkala
	M.1.4	*Continuous improvement* telah diterapkan dan berjalan efektif
	M.1.5	*Quality assurance* telah diterapkan dan berjalan efektif
Operations & Facilities	M.2.1	*SOC exercise* dilaksanakan secara berkala
	M.2.2	Hasil *SOC exercise* digunakan untuk meningkatkan kemampuan kesiapan dan operasional SOC
	M.2.3	Operasional SOC distandarisasi melalui pertemuan dan prosedur
	M.2.4	Fasilitas fisik SOC tersedia dan berfungsi efektif dalam mendukung karyawan SOC
	M.2.5	Jadwal kerja (termasuk *stand-by* jika berlaku) diimplementasikan dan dioptimalkan
Reporting & Communication	M.3.1	Program *metrics* SOC telah diterapkan
	M.3.2	Proses pelaporan SOC diterapkan dan berjalan efektif
	M.3.3	Isi laporan SOC disetujui oleh *stakeholder* yang relevan
	M.3.4	*Vulnerability* dan *threat advisories* disampaikan ke *stakeholder* yang relevan
	M.3.5	Komunikasi SOC distandarisasi dan dioptimalkan
Use Case Management	M.4.1	Proses *use case management* didokumentasikan, diterapkan, dan berjalan efektif
	M.4.2	Efektivitas dan kualitas *use case* telah diukur
	M.4.3	Analisis MITRE ATT&CK® dilakukan untuk menentukan relevansi dan memprioritaskan teknik serangan
	M.4.4	MITRE ATT&CK® digunakan untuk mengoptimalkan cakupan deteksi
	M.4.5	*Visibility* telah dipahami dan ditingkatkan
Detection Engineering & Validation	M.5.1	Proses *detection engineering* didokumentasikan, diterapkan, dan berjalan efektif
	M.5.2	*Detection engineering* berkolaborasi dengan analis CTI dan analis SOC untuk tujuan optimasi
	M.5.3	Perubahan/pembaruan *detection rules* terkontrol
	M.5.4	*Detection rules* diuji saat penerapan
	M.5.5	*Detection rules* diuji dalam operasional menggunakan berbagai teknik

4. Domain *Technology*

Tabel 5. Daftar Pertanyaan FGD (Domain *Technology*)

Subkategori	Kode	Pertanyaan
SIEM / UEBA	T.1.1	*Ownership* teknologi SIEM/UEBA telah ditetapkan
	T.1.2	Teknologi SIEM/UEBA didokumentasikan secara fungsional dan teknis
	T.1.3	Teknologi SIEM/UEBA dikontrol dan dipelihara oleh personel terlatih
	T.1.4	Keberlanjutan dan ketersediaan teknologi SIEM/UEBA telah dikelola

	T.1.5	Akses ke perangkat SIEM/UEBA dikontrol dan diverifikasi
	T.1.6	Fungsi inti SIEM/UEBA telah diterapkan dan dioptimalkan
	T.1.7	Pengumpulan data telah diterapkan dan berjalan efektif
	T.1.8	Integrasi teknis dan proses telah diterapkan
	T.1.9	Deteksi berbasis anomali dan *rule-based* diterapkan dan berjalan efektif dalam mendeteksi insiden
	T.1.10	Visualisasi dan laporan diterapkan dan efektif dalam mendukung analisis
NDR	T.2.1	*Ownership* teknologi NDR telah ditetapkan
	T.2.2	Teknologi NDR didokumentasikan secara fungsional dan teknis
	T.2.3	Teknologi NDR dikontrol dan dipelihara oleh personel terlatih
	T.2.4	Keberlanjutan dan ketersediaan teknologi NDR telah dikelola
	T.2.5	Akses ke perangkat NDR dikontrol dan diverifikasi
	T.2.6	Fungsi inti NDR telah diterapkan dan dioptimalkan
	T.2.7	Pengumpulan dan pemrosesan data telah diterapkan dan berjalan efektif
	T.2.8	Integrasi teknis dan proses telah diterapkan
	T.2.9	Deteksi berbasis anomali dan *rule-based* diterapkan dan berjalan efektif dalam mendeteksi insiden
	T.2.10	Visualisasi dan laporan diterapkan dan efektif dalam mendukung analisis
EDR	T.3.1	*Ownership* teknologi EDR telah ditetapkan
	T.3.2	Teknologi EDR didokumentasikan secara fungsional dan teknis
	T.3.3	Teknologi EDR dikontrol dan dipelihara oleh personel terlatih
	T.3.4	Keberlanjutan dan ketersediaan teknologi EDR telah dikelola
	T.3.5	Akses ke perangkat EDR dikontrol dan diverifikasi
	T.3.6	Fungsi inti EDR telah diterapkan dan dioptimalkan
	T.3.7	Kapabilitas deteksi diterapkan dan berjalan efektif dalam mendeteksi insiden
	T.3.8	Kapabilitas respon diterapkan dan berjalan efektif dalam mitigasi insiden
	T.3.9	Integrasi teknis dan proses telah diterapkan
	T.3.10	Visualisasi dan laporan diterapkan dan efektif dalam mendukung analisis
SOAR	T.4.1	*Ownership* teknologi SOAR telah ditetapkan
	T.4.2	Teknologi SOAR didokumentasikan secara fungsional dan teknis
	T.4.3	Teknologi SOAR dikontrol dan dipelihara oleh personel terlatih
	T.4.4	Keberlanjutan dan ketersediaan teknologi SOAR telah dikelola
	T.4.5	Akses ke perangkat SOAR dikontrol dan diverifikasi
	T.4.6	Fungsi inti SOAR telah diterapkan dan dioptimalkan
	T.4.7	*Playbook automations* diterapkan dan berjalan efektif
	T.4.8	*Automated responses* diterapkan dan berjalan efektif dalam meningkatkan efisiensi SOC
	T.4.9	Integrasi teknis dan proses telah diterapkan
	T.4.10	Visualisasi dan laporan diterapkan dan efektif dalam mendukung analisis

5. Domain *Services*

Tabel 6. Daftar Pertanyaan FGD (Domain *Services*)

Subkategori	Kode	Pertanyaan
Security Monitoring	S.1.1	*Security monitoring service* didokumentasikan
	S.1.2	*Security monitoring service* beroperasi dan berjalan efektif
	S.1.3	Pelaksanaan *security monitoring service* distandarisasi melalui prosedur

	S.1.4	*Security monitoring service* diukur dengan menggunakan KPI dan target yang telah ditetapkan
	S.1.5	*Security monitoring service* ditingkatkan secara berkelanjutan
	S.1.6	*False-positives* dikelola dan dikurangi secara efektif
	S.1.7	*Security monitoring* mampu mendeteksi ancaman pada seluruh tahapan *attack chain*
	S.1.8	*Security monitoring* mampu mendeteksi ancaman pada berbagai tipe aset
	S.1.9	Analisis *security alerts* dilaksanakan secara terstandarisasi dan efektif
	S.1.10	Cakupan *security monitoring* diukur dan ditingkatkan secara aktif
	S.2.1	*Security incident management service* didokumentasikan
	S.2.2	*Security incident management service* beroperasi dan berjalan efektif
	S.2.3	Pelaksanaan *security incident management service* distandarisasi melalui prosedur
	S.2.4	*Security incident management service* diukur dengan KPI dan target yang ditetapkan
Security Incident Management	S.2.5	*Security incident management service* ditingkatkan secara berkelanjutan
	S.2.6	Insiden ditangani secara terstandarisasi, efisien, dan efektif
	S.2.7	*Incident escalation* dilakukan melalui proses standar dengan jalur eskalasi yang ditentukan
	S.2.8	Strategi mitigasi insiden dipahami dan distandarisasi
	S.2.9	*Lessons learned* diambil dari insiden secara terstandarisasi
	S.2.10	Prosedur pemulihan telah diterapkan dan berjalan efektif, termasuk validasi aset yang dipulihkan
	S.3.1	*Security analysis & forensics service* didokumentasikan
	S.3.2	*Security analysis & forensics service* beroperasi dan berjalan efektif
	S.3.3	Pelaksanaan *security analysis & forensics service* distandarisasi melalui prosedur
	S.3.4	*Security analysis & forensics service* diukur dengan KPI dan target yang telah ditetapkan
Security Analysis & Forensics	S.3.5	*Security analysis & forensics service* ditingkatkan secara berkelanjutan
	S.3.6	*Hardware* dan *software* forensik tersedia dan dioptimalkan
	S.3.7	Prosedur pengumpulan bukti ditetapkan untuk menjaga integritas *chain of custody*
	S.3.8	Analisis forensik terhadap sistem dilaksanakan
	S.3.9	Analisis forensik terhadap malware dilaksanakan
	S.3.10	Analisis forensik terhadap jaringan dilaksanakan
	S.4.1	*Threat intelligence service* didokumentasikan
	S.4.2	*Threat intelligence service* beroperasi dan berjalan efektif
	S.4.3	Pelaksanaan *threat intelligence service* distandarisasi melalui prosedur
	S.4.4	*Threat intelligence service* diukur dengan KPI dan target yang telah ditetapkan
Threat Intelligence	S.4.5	*Threat intelligence service* ditingkatkan secara berkelanjutan
	S.4.6	CTI dikumpulkan dari sumber yang dikelola
	S.4.7	CTI dianalisis secara terstandarisasi dan efektif
	S.4.8	CTI yang telah dianalisis digunakan untuk memberikan informasi yang dapat ditindaklanjuti kepada pemangku kepentingan
	S.4.9	CTI disebarluaskan dengan format standar industri
	S.4.10	*Threat intelligence platform* dikelola dan dioptimalkan
Threat Hunting	S.5.1	*Threat hunting service* didokumentasikan
	S.5.2	*Threat hunting service* beroperasi dan berjalan efektif

	S.5.3	Pelaksanaan *threat hunting service* distandarisasi melalui prosedur
	S.5.4	*Threat hunting service* diukur dengan KPI dan target yang telah ditetapkan
	S.5.5	*Threat hunting service* ditingkatkan secara berkelanjutan
	S.5.6	Investigasi *threat hunting* dilakukan dengan metodologi yang telah ditetapkan
	S.5.7	*Threat hunting* dilakukan terhadap IoC
	S.5.8	*Threat hunting* dilakukan terhadap *tools* dan artefak *host/network*
	S.5.9	*Threat hunting* dilakukan terhadap TTP
	S.5.10	Laporan investigasi *threat hunting* dibuat dan memuat rekomendasi peningkatan deteksi
	S.6.1	*Vulnerability management service* didokumentasikan
	S.6.2	*Vulnerability management service* beroperasi dan berjalan efektif
	S.6.3	Pelaksanaan *vulnerability management service* distandarisasi melalui prosedur
	S.6.4	*Vulnerability management service* diukur dengan KPI dan target yang telah ditetapkan
	S.6.5	*Vulnerability management service* ditingkatkan secara berkelanjutan
Vulnerability Management	S.6.6	*Vulnerability scanning* dilaksanakan secara berkala pada aset IT yang relevan
	S.6.7	Hasil *vulnerability scanning* dianalisis dan diprioritaskan
	S.6.8	Tren kerentanan diidentifikasi dan ditindaklanjuti
	S.6.9	Laporan kerentanan berisi informasi yang dapat ditindaklanjuti dikirimkan kepada pemangku kepentingan
	S.6.10	Cakupan manajemen kerentanan diukur dan ditingkatkan secara aktif
	S.7.1	*Log management service* didokumentasikan
	S.7.2	*Log management service* beroperasi dan berjalan efektif
	S.7.3	Pelaksanaan *log management service* distandarisasi melalui prosedur
	S.7.4	*Log management service* diukur dengan KPI dan target yang telah ditetapkan
Log Management	S.7.5	*Log management service* ditingkatkan secara berkelanjutan
	S.7.6	*Logging* dikumpulkan melalui transfer yang aman
	S.7.7	*Logging* dinormalisasi dan diagregasi untuk mengoptimalkan pencarian dan penyimpanan
	S.7.8	Retensi *logging* diterapkan sesuai dengan kebijakan dan regulasi
	S.7.9	Akses terhadap *logging* dibatasi dan dikelola
	S.7.10	*Log archiving* diterapkan dan berjalan efektif

II. *Suggestion* / Definisi Tujuan

Berdasarkan *gap* yang telah teridentifikasi, dilakukan *mapping gap* tersebut ke framework NIST CSF 2.0 dan domain SOC-CMM untuk mengetahui aspek NIST CSF apa saja yang belum dipenuhi oleh tim SOC, serta aktivitas apa saja yang perlu dilakukan untuk memenuhi *gap* aspek tersebut.

III. Design dan Pengembangan *Artifact*

Daftar aktivitas yang telah diidentifikasi kemudian disusun menjadi rancangan kapabilitas dalam bentuk rekomendasi praktis yang dapat dilakukan oleh PT. XYZ dengan referensi *best practice* industri yang relevan.

C. Hasil dan Pembahasan

Tahap 1: Identifikasi Kebutuhan

Kebutuhan perusahaan terkait pemantauan keamanan *public cloud environment* telah digambarkan secara eksplisit dalam dokumen *management review* Divisi *Information Security* PT. XYZ tahun 2024. Salah satu isu utama yang menjadi perhatian top *management* dalam tinjauan tersebut adalah belum optimalnya kapabilitas monitoring terhadap aset perusahaan yang berada di *cloud environment*..

Sebagai langkah awal pengembangan kapabilitas, dilakukan proses identifikasi kesenjangan (gap) antara kondisi kapabilitas tim SOC saat ini dengan kapabilitas yang dibutuhkan untuk melakukan *monitoring* terhadap *public cloud*. Untuk mendukung proses ini, digunakan instrumen SOC-CMM screening tool, yang telah banyak digunakan dalam literatur dan praktik untuk menilai kapabilitas operasional SOC secara menyeluruh [9].

Penilaian dilakukan terhadap seluruh domain dalam kerangka SOC-CMM, yaitu: *Strategy, Governance, Process, People, Technology, dan Services*. Pengecualian dilakukan terhadap subdomain *Vulnerability Management* pada domain *Services*, yang berada di luar ruang lingkup fungsi SOC pada PT. XYZ karena ditangani oleh tim terpisah dalam struktur organisasi.

Hasil dari proses identifikasi gap kemudian dikelompokkan berdasarkan domain dalam SOC-CMM. Setiap domain dianalisis untuk melihat kondisi eksisting dan perbandingannya terhadap kondisi ideal yang dibutuhkan untuk mendukung pemantauan lingkungan *public cloud* secara optimal. Tabel 7 berikut merangkum hasil identifikasi tersebut:

Tabel 7. *Gap* Kapabilitas Tim SOC dalam *Monitoring Environment Public Cloud*

Kode	Kode Pertanyaan	Gap
GAP-01	B.2.1	*Stakeholder* yang terkait dengan *public cloud* belum teridentifikasi
GAP-02	B.2.2	*Stakeholder* yang terkait dengan *public cloud* belum terdokumentasi
GAP-03	B.2.3	Ekspektasi terhadap *stakeholder* yang terkait dengan operasional *public cloud* belum terdokumentasi
GAP-04	B.5.1	Kebijakan terkait aktivitas SOC di *public cloud environment* belum tersedia secara komprehensif
GAP-05	P.2.3	Tanggung jawab terhadap *monitoring public cloud environment* belum di-*designate* ke roles tim SOC
GAP-06	P.4.1	*Knowledge* yang dimiliki tim SOC (*asset list, playbook, ruleset, password manager*) belum mencakup *knowledge* terkait *cloud monitoring*
GAP-07	P.4.4	Belum tersedia *knowledge/skill matrix* terkait *cloud monitoring*
GAP-08	P.4.5	Penggunaan *knowledge/skill requirements* terkait *cloud monitoring* belum dilakukan karena belum tersedianya *knowledge/skill matrix* terkait *cloud monitoring*
GAP-09	P.5.1	Belum ada *training* terkait *cloud monitoring* bagi tim SOC
GAP-10	P.5.2	Belum tersedia program sertifikasi terkait *cloud monitoring* bagi tim SOC
GAP-11	M.4.1	Belum terdapat *use case cloud monitoring* bagi tim SOC
GAP-12	M.2.1	Belum pernah dilakukan SOC *exercise* untuk menguji kemampuan *cloud monitoring*
GAP-13	M.4.5	Belum dilakukan *review visibility* tim SOC terhadap *public cloud environment*

GAP-14	M.5.1	Belum ada *review* proses *detection engineering* dalam *monitoring cloud*
GAP-15	M.5.3	Tim SOC tidak melakukan *changes/updates* ke *detection rules* terkait *public cloud environment*
GAP-16	M.5.4, M.5.5	Kegiatan pengujian kapabilitas deteksi di *public cloud environment* belum dilakukan
GAP-17	T.1.1, T.1.2, T.1.3, T.1.4, T.1.5, T.1.6, T.1.7, T.1.8, T.1.9, T.1.10	Tim SOC belum memiliki akses ke teknologi SIEM pada *public cloud environment*
GAP-18	T.2.1, T.2.2, T.2.3, T.2.4, T.2.5, T.2.6, T.2.7, T.2.8, T.2.9, T.2.10	Tim SOC belum memiliki akses ke teknologi NDR pada *public cloud environment*
GAP-19	T.3.1, T.3.2, T.3.3, T.3.4, T.3.5, T.3.6, T.3.7, T.3.8, T.3.9, T.3.10	Tim SOC belum memiliki akses ke teknologi EDR pada *public cloud environment*
GAP-20	T.4.1, T.4.2, T.4.3, T.4.4, T.4.5, T.4.6, T.4.7, T.4.8, T.4.9, T.4.10	Tim SOC belum memiliki akses ke teknologi SOAR pada *public cloud environment*
GAP-21	S.1.2	Aktivitas *security monitoring* belum berjalan secara efektif pada *public cloud environment*
GAP-22	S.1.7	Tim SOC belum dapat mendeteksi semua aspek *attack chain* pada *public cloud environment*
GAP-23	S.1.8	Tim SOC belum dapat mendeteksi ancaman pada semua jenis aset *public cloud environment*
GAP-24	S.1.9	Analisis *security alerts* belum dilakukan secara efektif akibat belum tersedianya tiket deteksi dan *playbook* pada *public cloud environment*
GAP-25	S.2.2	Manajemen insiden *security* belum dijalankan secara efektif pada *public cloud environment*
GAP-26	S.2.3, S.2.6, S.2.8	Prosedur tanggap insiden pada *public cloud environment* belum tersedia
GAP-27	S.2.7	Prosedur respon insiden saat ini belum mendefinisikan eskalasi ke CSP
GAP-28	S.2.10	Tim SOC belum memiliki dan/atau menjalankan prosedur *recovery* insiden pada *public cloud environment*
GAP-29	S.3.2	Aktivitas analisis dan forensik belum dilakukan secara efektif pada *public cloud environment*
GAP-30	S.3.3, S.3.7	Belum ada penyesuaian prosedur forensik untuk *cloud*
GAP-31	S.3.6	*Tools* forensik untuk *cloud* belum tersedia
GAP-32	S.4.2	Kegiatan *threat intelligence* belum dijalankan secara efektif pada *public cloud* environment
GAP-33	S.4.3	Belum ada penyesuaian prosedur *threat intelligence* untuk *cloud*
GAP-34	S.4.6	Tim SOC belum mengumpulkan *threat intelligence* terkait *public cloud environment*
GAP-35	S.4.10	Tim SOC belum menggunakan *platform* yang dapat me-*manage threat intelligence* pada *public cloud environment*
GAP-36	S.5.2	Kegiatan *threat hunting* belum dijalankan secara efektif pada *public cloud environment*

GAP-37	S.5.3	Belum ada penyesuaian prosedur *threat hunting* untuk *public cloud environment*
GAP-38	S.5.6	Metodologi *threat hunting* belum disesuaikan untuk *threat hunting* pada *public cloud environment*
GAP-39	S.5.7	*Threat hunting* berdasarkan IoC belum dilakukan secara efektif pada *public cloud environment*
GAP-40	S.5.8	*Threat hunting* belum dilakukan terhadap *artifact host/network* pada *public cloud environment*
GAP-41	S.5.9	*Threat hunting* berdasarkan TTP belum dilakukan secara efektif pada *public cloud environment*
GAP-42	S.7.1	Ketentuan *log management* tersedia di berbagai ketentuan (di SOP Kegiatan Fungsi SOC, *job description System Engineer*, dll), namun saat ini belum ada penyesuaian untuk *logging* pada *public cloud environment*
GAP-43	S.7.6	Pengumpulan *log* pada *public cloud environment* belum dilakukan
GAP-44	S.7.7	Normalisasi dan agregasi *log* belum dilakukan pada *public cloud environment*
GAP-45	S.7.8	Retensi *logging* pada *public cloud environment* belum disesuaikan dengan ketentuan yang berlaku
GAP-46	S.7.10	Proses *log archiving* pada *public cloud environment* belum terimplementasi

Tahap 2: *Suggestion* / Definisi Tujuan

Setelah proses identifikasi *gap* kapabilitas, dilakukan pemetaan lebih lanjut terhadap subkategori pada kerangka kerja NIST *Cybersecurity Framework* (CSF) versi 2.0 untuk menentukan tujuan pengembangan kapabilitas SOC. NIST CSF 2.0 merupakan kerangka kerja manajemen risiko keamanan siber yang memuat enam fungsi utama (*Govern, Identify, Protect, Detect, Respond,* dan *Recover*) yang dijabarkan dalam 22 kategori dan 106 subkategori. *Framework* ini dapat digunakan untuk menilai *outcome* yang seharusnya dicapai oleh organisasi dalam menjalankan pengelolaan keamanan siber [11]. Berdasarkan hasil pemetaan, ditemukan bahwa terdapat 54 subkategori NIST CSF yang belum terpenuhi oleh tim SOC PT. XYZ dalam konteks pemantauan *public cloud environment*. Masing-masing subkategori tersebut kemudian dipetakan ke dalam domain-domain yang relevan pada SOC-CMM guna mengidentifikasi area kapabilitas yang perlu dikembangkan.

Hasil pemetaan tersebut menunjukkan bahwa dibutuhkan 71 aktivitas kapabilitas tambahan yang tersebar di lima domain utama SOC-CMM, yaitu *Business, People, Process, Technology,* dan *Services*. Jumlah aktivitas ini lebih banyak dibandingkan jumlah subkategori karena satu subkategori dapat mencerminkan kebutuhan di lebih dari satu domain kapabilitas.

Tabel 8. *Gap* Kapabilitas Tim SOC dalam *Monitoring Environment Cloud*

Subkategori NIST CSF	Domain	Kode	Aktivitas	Referensi Gap
GV.OC-02	*Business*	A-01	Mengidentifikasi *stakeholder* yang terkait dengan *cloud computing*, beserta kebutuhan dan ekspektasinya masing-masing	GAP-01, GAP-02, GAP-03
GV.OC-03	*Services*	A-02	Menetapkan dan mengevaluasi ketentuan retensi *log* pada *public cloud*	GAP-45, GAP-46

Subkategori NIST CSF	Domain	Kode	Aktivitas	Referensi Gap
GV.OC-04	*Business*	A-03	Menyusun dan me*review* dokumentasi *Shared Service Responsibility* dengan masing-masing CSP	GAP-03
GV.RR-02	*People*	A-04	Memperbarui tugas dan tanggung jawab masing-masing personil tim SOC dalam menjalankan kegiatan tim SOC pada *public cloud*	GAP-05
GV.RR-02	*Technology*	A-05	Menyusun ketentuan terkait *ownership* teknologi tim SOC pada *public cloud*	GAP-17, GAP-18, GAP-19, GAP-20
GV.RR-03	*People*	A-06	Melakukan *management review* terkait penambahan *role* untuk kebutuhan *public cloud monitoring* sesuai *best practice* yang berlaku	GAP-05
GV.PO-01	*Business*	A-07	Menyusun kebijakan yang mendukung aktivitas tim SOC pada *public cloud* yang mencakup: *logging & monitoring, security incident management, threat intel, threat hunting*, dst	GAP-04
GV.PO-01	*Services*	A-08	Menyusun kebijakan *logging & monitoring* pada *public cloud* PT. XYZ, termasuk retensi data	GAP-42, GAP-45
GV.PO-02	*Business*	A-09	Mengesahkan kebijakan yang mendukung aktivitas tim SOC pada *public cloud* yang mencakup: *logging* & *monitoring, security incident management, threat intel, threat hunting*, dst	GAP-04
GV.SC-02	*Business*	A-10	Mengidentifikasi dan mendokumentasikan tanggung jawab tim SOC terhadap masing-masing *stakeholder cloud computing*	GAP-01, GAP-02
GV.SC-04	*Business*	A-11	Mengidentifikasi dan mendokumentasikan detil CSP (*Cloud Service Provider*) yang digunakan PT. XYZ	GAP-01, GAP-02
GV.SC-08	*Services*	A-12	Mengembangkan dan memelihara *incident response plan* yang mencakup: prosedur komunikasi dengan CSP, penggunaan layanan *incident response* masing-masing CSP	GAP-27
ID.AM-02	*Process*	A-13	Mengelola daftar aset dan *services* yang digunakan pada *public cloud* agar selalu tersedia dan *up-to-date*	GAP-13
ID.AM-03	*Process*	A-14	Menyusun dan memperbarui dokumentasi data *flow* yang mendeskripsikan data yang diproses, disimpan, dan ditransmisikan ke *public cloud*	GAP-13
ID.AM-03	*Technology*	A-15	Mengimplementasikan solusi keamanan yang dapat menganalisa alur komunikasi dan jaringan pada *public cloud*	GAP-18
ID.AM-04	*Business*	A-16	Mengidentifikasi dan mendokumentasikan seluruh layanan *public cloud* yang digunakan oleh PT. XYZ	GAP-01, GAP-02

Subkategori NIST CSF	Domain	Kode	Aktivitas	Referensi Gap
ID.AM-05	*Process*	A-17	Melengkapi daftar aset pada *public cloud* dengan konteks kritikalitas masing-masing aset	GAP-13
ID.RA-02	*Services*	A-18	Mengelola dan memperbarui *threat intelligence* yang relevan pada *public cloud* dari sumber terpercaya	GAP-32, GAP-33, GAP-34, GAP-35
ID.RA-03	*Services*	A-19	Melakukan pengelolaan ancaman melalui aktivitas *threat intelligence* dan *threat hunting*	GAP-32, GAP-34, GAP-36, GAP-37, GAP-38, GAP-39, GAP-41
ID.IM-02	*Process*	A-20	Menyelenggarakan SOC *exercise* secara rutin dengan melibatkan *stakeholder* terkait serta mendokumentasikan hasil dan *lesson learned*	GAP-12
ID.IM-03	*Process*	A-21	Menjalankan kegiatan *continuous improvement* pada keseluruhan operasional tim SOC	GAP-11, GAP-14, GAP-15, GAP-16
ID.IM-04	*Services*	A-22	Mengesahkan dan mengkomunikasikan prosedur operasional	GAP-26, GAP-30, GAP-42
PR.AA-03	*Technology*	A-23	Mengatur akses *tools security* pada *public cloud* agar hanya dapat diakses personel berwenang sesuai ketentuan	GAP-17, GAP-18, GAP-19, GAP-20
PR.AA-05	*Technology*	A-24	Mengatur dan me*review* akses ke *tools security* pada *public cloud* sesuai ketentuan dengan prinsip *least privilege* dan *separation of duty*	GAP-17, GAP-18, GAP-19, GAP-20
PR.AT-02	*People*	A-25	Mengidentifikasi *skill* dan *knowledge* yang diperlukan setiap *role* serta menyelenggarakan pelatihan sesuai kebutuhan	GAP-06, GAP-07, GAP-08, GAP-09, GAP-10
PR.AT-02	*Technology*	A-26	Memberikan pelatihan dan pengembangan pengetahuan bagi personel tim SOC untuk mengoperasikan *tools security* pada *public cloud*	GAP-17, GAP-18, GAP-19, GAP-20
PR.DS-02	*Services*	A-27	Mengatur pengiriman *log* dari *public cloud* menggunakan mekanisme yang *secure*	GAP-43
PR.DS-11	*Services*	A-28	Melakukan pengarsipan *log* sesuai ketentuan yang berlaku	GAP-46
PR.PS-01	*Technology*	A-29	Mengelola konfigurasi teknologi tim SOC di *public cloud* agar sesuai ketentuan dengan dokumentasi terkini	GAP-17, GAP-18, GAP-19, GAP-20
PR.PS-02	*Process*	A-30	Menyusun proses *detection engineering* untuk meningkatkan kemampuan deteksi teknologi tim SOC	GAP-14, GAP-16

Subkategori NIST CSF	Domain	Kode	Aktivitas	Referensi Gap
PR.PS-04	*Services*	A-31	Menyediakan dan memastikan kelengkapan *log* keamanan pada *public cloud*	GAP-44
PR.PS-04	*Technology*	A-32	Mengimplementasikan dan mengelola teknologi SIEM & NDR yang dapat menerima serta memantau log keamanan pada *public cloud*	GAP-17, GAP-18
PR.IR-03	*Technology*	A-33	Mengelola ketersediaan teknologi tim SOC pada *public cloud* secara optimal	GAP-17, GAP-18, GAP-19, GAP-20
PR.IR-04	*Technology*	A-34	Memastikan kapasitas teknologi tim SOC pada *public cloud* selalu tersedia sesuai kebutuhan	GAP-17, GAP-18, GAP-19, GAP-20
DE.CM-01	*Process*	A-35	Mendefinisikan proses pemantauan keamanan jaringan pada *public cloud*	GAP-11, GAP-14, GAP-15
DE.CM-01	*Technology*	A-36	Mengimplementasikan teknologi yang memiliki kapabilitas pemantauan jaringan pada *public cloud*	GAP-17, GAP-18
DE.CM-01	*Services*	A-37	Menjalankan kegiatan pemantauan jaringan pada *public cloud*	GAP-21, GAP-22, GAP-23, GAP-36, GAP-40
DE.CM-03	*Process*	A-38	Mendefinisikan proses pemantauan aktivitas pengguna pada *public cloud* melalui aktivitas tim SOC	GAP-11, GAP-14
DE.CM-03	*Technology*	A-39	Mengimplementasikan teknologi yang memiliki kapabilitas pemantauan aktivitas pengguna pada *public cloud*	GAP-17, GAP-18, GAP-19
DE.CM-03	*Services*	A-40	Menjalankan kegiatan pemantauan aktivitas pengguna pada *public cloud*	GAP-21, GAP-22, GAP-23, GAP-36, GAP-40
DE.CM-06	*Process*	A-41	Mendefinisikan proses pemantauan aktivitas sistem eksternal pada *public cloud* melalui aktivitas tim SOC	GAP-11, GAP-14
DE.CM-06	*Technology*	A-42	Mengimplementasikan teknologi yang dapat memantau aktivitas entitas eksternal pada *public cloud*	GAP-17, GAP-18, GAP-20
DE.CM-06	*Services*	A-43	Menjalankan kegiatan pemantauan aktivitas sistem eksternal pada *public cloud* melalui aktivitas tim SOC	GAP-21, GAP-22, GAP-23, GAP-40
DE.CM-09	*Services*	A-44	Menjalankan kegiatan pemantauan aset pada *public cloud* melalui aktivitas tim SOC	GAP-21, GAP-22, GAP-23, GAP-36, GAP-40
DE.CM-09	*Technology*	A-45	Mengimplementasikan teknologi yang memiliki kapabilitas pemantauan aset pada *public cloud*	GAP-17, GAP-19

Subkategori NIST CSF	Domain	Kode	Aktivitas	Referensi Gap
DE.CM-09	*Process*	A-46	Mendefinisikan proses pemantauan aset pada *public cloud* melalui aktivitas tim SOC	GAP-11, GAP-14, GAP-15
DE.AE-02	*Technology*	A-47	Mengimplementasikan teknologi yang memiliki kapabilitas analisa *security events* pada *public cloud*	GAP-17
DE.AE-02	*Services*	A-48	Menjalankan kegiatan analisa *security events* pada *public cloud* melalui aktivitas tim SOC	GAP-21, GAP-36, GAP-37, GAP-38, GAP-41
DE.AE-03	*Technology*	A-49	Mengimplementasikan teknologi yang memiliki kapabilitas korelasi informasi dari berbagai sumber	GAP-17, GAP-18, GAP-19, GAP-20
DE.AE-04	*Services*	A-50	Menjalankan aktivitas *triage* untuk mengetahui dampak dan ruang lingkup dari suatu *security event*	GAP-21
DE.AE-06	*Technology*	A-51	Mengimplementasikan teknologi yang dapat menyampaikan informasi *security* secara efektif melalui visualisasi dan *reports*	GAP-17, GAP-18, GAP-19, GAP-20
DE.AE-07	*Technology*	A-52	Mengimplementasikan teknologi yang dapat melakukan analisa *security events* pada *public cloud* yang terintegrasi dengan *threat intelligence*	GAP-17, GAP-18, GAP-19, GAP-20
DE.AE-07	*Services*	A-53	Mengintegrasikan *threat intelligence* dalam menjalankan kegiatan analisa *security events* pada *public cloud*	GAP-32, GAP-33, GAP-36, GAP-37, GAP-39, GAP-41
DE.AE-08	*Technology*	A-54	Mengimplementasikan teknologi yang dapat mendeteksi potensi insiden dari *security events*	GAP-17, GAP-18, GAP-19
RS.MA-01	*Services*	A-55	Menjalankan respon insiden dengan melibatkan pihak ketiga terkait	GAP-25
RS.MA-02	*Services*	A-56	Menjalankan *triage* dan validasi potensi insiden pada *public cloud*	GAP-24, GAP-25, GAP-26
RS.MA-03	*Services*	A-57	Menjalankan kategorisasi dan prioritisasi potensi insiden pada *public cloud*	GAP-24, GAP-25, GAP-26
RS.MA-04	*Services*	A-58	Menjalankan eskalasi potensi insiden pada *public cloud*	GAP-24, GAP-25, GAP-26
RS.MA-05	*Services*	A-59	Mendefinisikan dan menggunakan kriteria dalam menentukan kapan melakukan *recovery* insiden	GAP-25
RS.AN-03	*Services*	A-60	Menjalankan kegiatan investigasi dan *root cause analysis* saat menjalankan respon insiden pada *public cloud*	GAP-24, GAP-26, GAP-29, GAP-30, GAP-31

Subkategori NIST CSF	Domain	Kode	Aktivitas	Referensi Gap
RS.AN-06	*Services*	A-61	Mendokumentasikan semua kegiatan yang dilakukan tim saat menjalankan respon insiden	GAP-26, GAP-29, GAP-30
RS.AN-07	*Services*	A-62	Melakukan verifikasi keabsahan data saat menjalankan respon insiden	GAP-26, GAP-29, GAP-30
RS.AN-08	*Services*	A-63	Menganalisis ruang lingkup aset yang terdampak saat menjalankan respon insiden	GAP-26, GAP-29
RS.CO-02	*Services*	A-64	Memberikan notifikasi kepada *stakeholder* terkait saat terjadi insiden	GAP-25, GAP-26, GAP-27
RS.CO-03	*Services*	A-65	Memberikan informasi yang dibutuhkan kepada *stakeholder* terkait saat menjalankan respon insiden	GAP-25, GAP-26, GAP-27
RS.MI-01	*Technology*	A-66	Mengimplementasikan teknologi dengan kapabilitas *containment* pada *public cloud*	GAP-19, GAP-20
RS.MI-01	*Services*	A-67	Menjalankan proses *containment* saat respon insiden	GAP-26
RS.MI-02	*Technology*	A-68	Mengimplementasikan teknologi dengan kapabilitas penghapusan dampak insiden pada *public cloud*	GAP-19, GAP-20
RS.MI-02	*Services*	A-69	Melakukan pengamanan aset yang terdampak setelah menjalankan respon insiden	GAP-26
RC.RP-01	*Services*	A-70	Menginisasi proses *recovery* setelah respon insiden	GAP-28
RC.RP-02	*Services*	A-71	Mendukung proses *recovery* setelah respon insiden	GAP-28

Tahap 3: *Design* dan Pengembangan *Artifact*

Berdasarkan analisa di tahap 1 dan 2, ditemukan bahwa dalam kasus ini terdapat gap kapabilitas SOC yang cukup signifikan di masing-masing aspek SOC sebagai berikut:

- ***People***: Kurangnya personil yang memiliki kompetensi khusus *cloud security*.
- ***Process***: Belum adanya proses dan dokumentasi (SOP, *playbook*, *asset list*, dan lain-lain) yang terdefinisi dengan baik dalam hal *monitoring* dan *incident handling* pada *cloud environment.*
- ***Technology***: Keterbatasan visibilitas yang disebabkan belum tersedianya teknologi *monitoring* yang memadai pada *environment public cloud* perusahaan.

Selanjutnya dilakukan perancangan *artifact* dalam bentuk rekomendasi praktis sesuai tujuan awal. Dalam menyusun rekomendasi praktis, penelitian ini menggunakan beberapa literatur sebagai referensi *best practice* perancangan kapabilitas tim SOC, yaitu:

1. *11 Strategies of a World-Class Cybersecurity Operations Center* [12], yang membahas 11 strategi utama untuk meningkatkan kemampuan SOC, termasuk aplikasi yang relevan pada kasus *monitoring cloud*
2. *CSA Security Guidance for Critical Areas of Focus in Cloud Computing v5* [13], yang membahas aspek-aspek kritis dalam pengamanan *environment cloud computing* termasuk *security monitoring*.

Berikut merupakan rekomendasi praktis yang dapat diterapkan dalam studi kasus ini, yang dipetakan sesuai domain SOC-CMM:

1. Rekomendasi Peningkatan Kapabilitas pada Domain *Business*

Tabel 9. Rekomendasi Praktis Domain *Business*

Kode	Referensi Aktivitas	Rekomendasi Praktis
R.B-01	A-01, A-10	Menganalisa *stakeholder* internal dan eksternal terkait *cloud computing* dan mendokumentasikannya pada daftar *stakeholder existing*, beserta informasi kontak dan ekspektasi masing-masing
R.B-02	A-03, A-16	Mengkaji *Shared Service Responsibility Model* setiap layanan yang digunakan pada masing-masing *cloud provider*, dan mengatur *scope monitoring* tim SOC berdasarkan ketentuan tersebut
R.B-03	A-07, A-09	Menyusun dan mengesahkan prosedur-prosedur tambahan operasional tim SOC pada *environment cloud* sesuai alur dan ketentuan formalisasi prosedur perusahaan

2. Rekomendasi Peningkatan Kapabilitas pada Domain *People*

Tabel 10. Rekomendasi Praktis Domain *People*

Kode	Referensi Aktivitas	Rekomendasi Praktis
R.P-01	A-04	Memperbarui tugas dan tanggung jawab masing-masing *role* pada SOP internal dan kontrak *staff* eksternal sesuai RACI *chart* yang telah disusun
R.P-02		Menambahkan *role cloud detection engineer* sebagai posisi khusus yang diisi oleh staf eksternal sebagai bagian dari tim SOC eksternal
R.P-03	A-25	Menyusun *skill* dan *knowledge matrix* yang diperlukan dan memetakannya ke masing-masing *role*, sekaligus mengidentifikasi *gap* yang muncul.
R.P-04		Menyesuaikan *training/certification path* karyawan internal berdasarkan *skill* dan *knowledge matrix* yang telah diperbarui
R.P-05		Menyesuaikan *baseline requirements staff* eksternal di masing-masing *role* berdasarkan *skill* dan *knowledge matrix* yang telah diperbarui
R.P-06	A-06	Melaksanakan *management review* untuk mengkomunikasikan kebutuhan SDM tambahan yang telah diidentifikasi dengan *stakeholder* terkait
R.P-07		Menyesuaikan kontrak tim SOC eksternal berdasarkan *requirements* tambahan yang telah diidentifikasi.

3. Rekomendasi Peningkatan Kapabilitas pada Domain *Process*

Tabel 11. Rekomendasi Praktis Domain *Process*

Kode	Referensi Aktivitas	Rekomendasi Praktis
R.M-01	A-13, A-17	Berkoordinasi dengan tim *Cloud Security* untuk mengetahui daftar aset perusahaan di *public cloud environment* saat ini, serta prioritisasinya
R.M-02		Menyusun dan mengesahkan dan menjadwalkan *review* berkala terhadap IT asset *list* yang sudah dimiliki oleh tim SOC
R.M-03		Mengimplementasikan sistem yang dapat menyusun dan memperbarui inventori aset secara otomatis pada masing-masing *cloud*
R.M-04	A-14	Berkoordinasi dengan tim *Cloud Security* dan tim pengembang terkait untuk mendapatkan *high-level data flow overview* aplikasi-aplikasi perusahaan yang menggunakan *resource cloud*
R.M-05	A-20, A-21	Memaksimalkan kegiatan SOC *Exercise existing* (*tabletop exercise*, *cyber drill*, *red teaming*) dengan mengadopsi skenario terkait *cloud monitoring*
R.M-06	A-35, A-38, A-41, A-46	Memperbarui *playbook existing* tim SOC dengan *use-case*: *1.* Respon terhadap *security alert* terkait aset pada *environment cloud* *2.* Respon terhadap *security alert* terkait jaringan pada *environment cloud* 3. Respon terhadap *security alert* terkait *user activity pada environment cloud* 4. Respon terhadap *security alert* terkait anomali sistem eksternal pada *environment cloud*
R.M-07	A-30	Menyusun proses *detection engineering* termasuk prosedur teknisnya pada setiap *cloud provider*

4. Rekomendasi Peningkatan Kapabilitas pada Domain *Technology*

Tabel 12. Rekomendasi Praktis Domain *Technology*

Kode	Referensi Aktivitas	Rekomendasi Praktis
R.T-01	A-05, A-26, A-29, A-33, A-34	Melakukan implementasi teknologi pada *cloud environment* sesuai standar perusahaan
R.T-02	A-32, A-47, A-49,	Mengimplementasikan teknologi *log management* di masing-masing *cloud provider* sesuai *best practice*
R.T-03	A-52, A-54	Mengimplementasikan teknologi SIEM atau sejenisnya yang dapat mendeteksi *security events* di masing-masing *cloud provider*
R.T-04		Mengintegrasikan *threat intelligence existing* tim SOC dengan teknologi SIEM di masing-masing *cloud provider*

Kode	Referensi Aktivitas	Rekomendasi Praktis
R.T-05	A-15, A-36, A-39,	Identifikasi dan integrasi *log-log* yang diperlukan untuk melakukan *security monitoring* (aktivitas aset, jaringan, pengguna dan entitas eksternal) ke solusi *log management* masing-masing *cloud provider*
R.T-06	A-42, A-25	Mengidentifikasi teknologi tambahan yang perlu diimplementasikan jika *log cloud* saat ini tidak memadai untuk melakukan *security monitoring*
R.T-07	A-66, A-68	Memastikan tim SOC memiliki akses dengan *permission* yang memadai untuk melakukan respon insiden pada *cloud*, termasuk *containment* dan *eradication*.
R.T-08		Mengimplementasikan teknologi yang dapat melakukan respon terhadap insiden/potensi insiden seperti CDR (*Cloud Detection & Response*)
R.T-09		Memaksimalkan teknologi *existing* SOC (SOAR) untuk melakukan respon terhadap insiden/potensi insiden pada *cloud*
R.T-10		Mengidentifikasi teknologi tambahan yang perlu diimplementasikan jika teknologi saat ini ini tidak memadai untuk melakukan *security response*
R.T-11	A-23, A-24	Menyusun dan mengaplikasikan *user access matrix* ke teknologi SOC pada *public cloud computing environment*

5. Rekomendasi Peningkatan Kapabilitas pada Domain *Services*

Tabel 13. Rekomendasi Praktis Domain *Services*

Kode	Referensi Aktivitas	Rekomendasi Praktis
R.S-01	A-37, A-40, A-43, A-44, A-48, A-50	Memaksimalkan tim *security monitoring existing* untuk melakukan *monitoring* pada c*loud environment*
R.S-02	A-02, A-07, A-08, A-09, A-27, A-28,	Memaksimalkan tim *system engineering* untuk melakukan manajemen *log* pada *cloud environment*
R.S-03	A-31	Menyusun prosedur manajemen *log* pada masing-masing *environment cloud*
R.S-04	A-07,A-09, A-12, A-55, A-56, A-57, A-58, A-59, A-60, A-61, A-62, A-63, A-64, A-65, A-67, A-69, A-70, A-71	Menyesuaikan dokumen manajemen insiden siber dengan menyusun prosedur respon insiden pada *environment cloud* yang mencakup proses respon insiden pada *cloud* secara *end-to-end*
R.S-05	A-19, A-37, A-40, A-43, A-44, A-48, A-53	Memaksimalkan tim *threat hunting existing* untuk melakukan *monitoring* pada *cloud environmen*t
R.S-06		Menyesuaikan prosedur *threat hunting existing* dengan menambahkan prosedur *threat hunting* & *detection engineering* pada *environment cloud*

R.S-07	A-30	Menyusun proses *detection engineering* termasuk prosedur teknisnya pada setiap *cloud provider*

D. Simpulan

Penelitian ini menghasilkan rancangan kapabilitas *Security Operations Center* (SOC) PT. XYZ untuk memantau lingkungan *public cloud* secara komprehensif sesuai standar *best practice* industri sebagai respons terhadap meningkatnya kebutuhan pengamanan aset *digital* di *cloud*. Proses perancangan didasarkan pada pendekatan *Design Science Research Methodology* (DSRM).

Identifikasi *gap* dilakukan melalui FGD yang didasarkan pada *framework* SOC-CMM. Melalui FGD tersebut diketahui gambaran kapabilitas tim SOC saat ini dan area pengembangan yang dibutuhkan. Selanjutnya, perumusan kapabilitas dilakukan dengan menggunakan NIST *Cybersecurity Framework* (CSF) 2.0 sebagai dasar. Sebanyak 71 aktivitas telah diidentifikasi sebagai bagian dari kapabilitas SOC yang diperlukan dalam pemantauan *cloud*. Aktivitas-aktivitas tersebut dipetakan ke dalam domain SOC-CMM dan subkategori NIST CSF. Berdasarkan aktivitas tersebut kemudian dirumuskan rekomendasi praktis per domain SOC-CMM yang dapat diaplikasikan oleh PT. XYZ.

Secara teoritis, penelitian ini telah mendemonstrasikan penggunaan DSRM untuk mengembangkan kapabilitas sebuath tim SOC. Dalam menyusun kapabilitas tim SOC, *framework* SOC-CMM dapat digunakan untuk mengidentifikasi *gap* kapabilitas dalam sebuah tim SOC, sedangkan *framework* NIST CSF dapat digunakan sebagai acuan untuk menghasilkan rancangan yang komprehensif.

E. Referensi

[1] Otoritas Jasa Keuangan, *Penyelenggaraan Teknologi Informasi oleh Bank Umum*, vol. 11/POJK.03/2022. 2022.

[2] International Monetary Fund, *Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks*. Washington, D.C.: International Monetary Fund, 2024. doi: 10.5089/9798400257704.082.

[3] I. A. Bajwa, S. Ahmad, M. Mahmud, and F. A. Bajwa, "The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector," *Inf. Comput. Secur.*, vol. 31, no. 5, pp. 635–654, Nov. 2023, doi: 10.1108/ICS-11-2022-0179.

[4] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," *IEEE Access*, vol. 8, pp. 227756–227779, 2020, doi: 10.1109/ACCESS.2020.3045514.

[5] *NIST SP 800-145, The NIST Definition of Cloud Computing*, Sep. 2011.

[6] S. Amamou, Z. Trifa, and M. Khmakhem, "Data protection in cloud computing: A Survey of the State-of-Art," *Procedia Comput. Sci.*, vol. 159, pp. 155–161, 2019, doi: 10.1016/j.procs.2019.09.170.

[7] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[8] J. M. Novak, A. L. Hueca, C. I. Rodman, S. Perl, J. Valdengo, and T. Breaux, "Building a Better SOC: Towards the Ontology for Security Operations Center

Assistance and Replication (OSCAR)," *Digit. Threats Res. Pract.*, p. 3722233, Mar. 2025, doi: 10.1145/3722233.
[9] SOC-CMM, "SOC-CMM Screening Tool." Accessed: May 25, 2025. [Online]. Available: https://www.soc-cmm.com/products/screening/
[10] R. van Os, "SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers," Lulea University of Technology, 2016.
[11] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
[12] K. Knerler, I. Parker, and C. Zimmerman, *11 Strategies of a world-class cybersecurity operations center / Kathryn Knerler, Ingred Parker, Carson Zimmerman*, Second edition. Bedford, Massachusetts: MITRE, 2023.
[13] Cloud Security Alliance, "CSA Security Guidance For Critical Areas of Focus in Cloud Computing v5," 2025.