CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 7, No. 2, November 2024, hlm. 95-110

Perancangan Tim Security Operation Center Di Perusahaan Sektor Finansial: Studi Kasus Dan Analisis

Farel Van Tony[1], Setiadi Yazid[2]

[1,2] Fakultas Ilmu Komputer, Universitas Indonesia
Email: [1]farel.van@ui.ac.id, [2]setiadi@cs.ui.ac.id

Abstrak

Tujuan penelitian ini untuk mengetahui perancangan tim security operation center di perusahaan sektor finansial. Keamanan informasi merupakan aspek penting dalam operasional perusahaan sektor finansial yang menangani data sensitif dan pengelolaan risiko global. Tim Security Operations Center (SOC) memainkan peran kunci dalam mendeteksi, menanggapi, dan mencegah serangan siber yang dapat mengganggu stabilitas keuangan. Penelitian ini mengadopsi pendekatan kualitatif deskriptif Penelitian ini bertujuan untuk mengembangkan model perancangan Tim SOC yang efektif di perusahaan sektor finansial. Studi kasus pada perusahaan XYZ menunjukkan bahwa faktor-faktor seperti pengalaman dan kepemimpinan, komunikasi dan kerja sama, teknologi dan alat kritis, serta dukungan manajemen sangat mempengaruhi kesuksesan operasional SOC. Pengelolaan SOC dalam konteks industri cryptocurrency yang memiliki risiko dan dinamika berbeda dari sektor lainnya. Hasil penelitian menunjukkan bahwa pemahaman mendalam tentang ancaman spesifik dan adaptasi terhadap regulasi yang ketat diperlukan untuk meningkatkan kinerja SOC. Dengan demikian, penelitian ini memberikan panduan untuk optimalisasi dan peningkatan efektivitas Tim SOC dalam menghadapi tantangan keamanan di lingkungan bisnis finansial.

Kata kunci: *keamanan informasi, tim security operation center (SOC), sektor finansial, kinerja operasional, stabilitas keuangan*

Designing Security Operations Center Team In Financial Sector Company: Sace Study And Analysis

Abstract

The purpose of this study was to determine the design of the security operation center team in financial sector companies. Information security is an important aspect of the operations of financial sector companies that handle sensitive data and manage global risks. Security Operations Center (SOC) teams play a key role in detecting, responding to, and preventing cyberattacks that can disrupt financial stability. This research adopts a descriptive qualitative approach This research aims to develop an effective SOC Team design model in financial sector companies. The case study of XYZ company shows that factors such as experience and leadership, communication and cooperation, critical technologies and tools, and management support greatly influence the operational success of the SOC. SOC management in the context of the cryptocurrency industry, which has different risks and dynamics from other sectors. The results show that an in-depth understanding of specific threats and adaptation to strict regulations are required to improve SOC performance. Thus, this research provides guidance for optimizing and improving the effectiveness of the SOC Team in facing security challenges in the financial business environment.

Keywords: *information security, security operations center (SOC) team, financial sector, operational performance, financial stability*

1. PENDAHULUAN

Industri finansial menjadi tulang punggung dalam mengalokasikan sumber daya keuangan di seluruh dunia (Mirza, 2021). Sebagai sektor yang mencakup perbankan, asuransi, lembaga keuangan non-bank, dan pasar modal, industri ini tidak hanya menangani investasi, tetapi juga pengelolaan risiko secara global. Keamanan informasi memiliki peran utama di sektor finansial karena sektor ini menyimpan data pribadi sensitif dan informasi keuangan yang krusial. Ancaman terhadap keamanan, seperti serangan siber dan pencurian identitas, dapat mengguncang fondasi kepercayaan dan stabilitas keuangan global.

Keamanan informasi menjadi prioritas di sektor finansial karena melibatkan penyimpanan dan perlindungan data sensitif nasabah dan perusahaan (Pakpahan, Elvira et al., 2020). Ini mencakup upaya untuk mencegah akses yang tidak sah dan memastikan integritas informasi. SOC memiliki peran krusial dalam memastikan

keamanan perusahaan finansial dengan memantau, mendeteksi, dan merespons ancaman keamanan serta memastikan keandalan sistem keamanan (Santoso, Murti, Adi & Nada, 2022). Mereka juga bertanggung jawab dalam menjaga layanan keuangan tetap tersedia dan terlindungi. Sektor finansial menghadapi tantangan keamanan unik, seperti regulasi yang ketat, volume transaksi yang besar, dan menjadi target utama bagi penjahat siber karena sensitivitas data yang tinggi. Keberhasilan SOC dalam menghadapi tantangan-tantangan ini menjadi kunci bagi keberlanjutan operasional perusahaan.

Dalam menanggapi tantangan keamanan yang semakin kompleks, keberlanjutan operasional *cryptocurrency exchange* menjadi kunci dalam mendukung evolusi sektor finansial (Putri Rizkia Wardhani, 2023). Dengan regulasi yang semakin ketat, volume transaksi besar, anonimitas, dan peningkatan risiko serangan siber, *cryptocurrency exchange* menjadi target utama bagi pelaku kejahatan siber yang mengincar data sensitif dan keuangan. Tim SOC tidak hanya perlu menghadapi ancaman yang sudah ada, tetapi juga harus mampu beradaptasi dengan tren dan teknologi baru dalam ekosistem *cryptocurrency*. Penerapan teknologi *blockchain* yang mendasari mata uang *crypto* memerlukan pemahaman mendalam dan pengelolaan keamanan yang efektif. Oleh karena itu, kemampuan SOC dalam menyelaraskan strategi keamanan dengan dinamika industri finansial dan *cryptocurrency exchange* akan menentukan tingkat keberhasilan dan ketahanan perusahaan di era digital ini. Keberlanjutan operasional dan integritas keamanan dalam *cryptocurrency exchange* menjadi prioritas utama yang mendukung eksistensi dan pertumbuhan sektor finansial yang semakin terintegrasi dengan dunia digital.

Pada Tahun 2023, perusahaan XYZ mengalami serangan siber yang berdampak pada kerugian finansial dan reputasi, banyak hal yang mendasari terjadinya insiden ini mulai dari salah konfigurasi dari sisi sistem internal, personel SOC yang tidak siap, kurangnya alat pendeteksi serangan, kurangnya dukungan manajemen terhadap tim SOC. Hal ini juga mendasari adanya konflik antara manajemen atas dan personel SOC, personel tim SOC menganggap bahwa manajemen atas hanya mementingkan kebutuhan unit bisnis saja sedangkan manajemen atas menginginkan hasil nyata yang bisa dihitung dari tim SOC. Namun, setelah kejadian insiden siber manajemen atas mulai menyadari betapa pentingnya kesuksesan tim SOC bagi perusahaan, sehingga dukungan mulai bertambah untuk tim SOC mencapai target mengamankan perusahaan.

Setelah insiden tersebut, Bank Sentral melakukan audit terhadap perusahaan XYZ dan tim audit internal melakukan audit berbasis standar ISO/IEC 27035-1:2016 untuk mengidentifikasi penyebab mendasar dari kegagalan sistem keamanan. Audit ini mengungkapkan sejumlah temuan penting yang perlu segera ditangani. Salah satunya adalah absennya dokumentasi formal *Information Security Incident Response Team* (ISIRT) yang seharusnya menjadi komponen vital dalam merespons insiden keamanan secara terstruktur. Selain itu, ditemukan bahwa pemantauan terhadap sistem kritis perusahaan masih sangat minim, sehingga meningkatkan risiko keterlambatan dalam mendeteksi ancaman. Audit juga menunjukkan rendahnya keterlibatan manajemen dalam proses pengelolaan keamanan informasi, serta kurangnya pengujian sistem insiden secara berkala, yang menyebabkan perusahaan tidak siap dalam menghadapi ancaman siber yang semakin kompleks.

Hasil wawancara lebih lanjut dengan pemangku kepentingan internal perusahaan mengungkapkan masalah lain yang turut memperburuk situasi. Kurangnya pengalaman kepemimpinan dalam tim SOC dan komunikasi yang lemah antar divisi perusahaan menjadi penghalang dalam penanganan insiden keamanan secara efektif. Selain itu, keterbatasan investasi, kekurangan tenaga kerja, serta teknologi *monitoring* yang tidak memadai semakin menghambat performa tim SOC. Faktor-faktor ini diperburuk oleh rendahnya pelatihan keterampilan bagi personel SOC, sehingga kemampuan tim untuk menghadapi ancaman modern menjadi terbatas. Di sisi lain, ancaman eksternal yang terus meningkat di industri *cryptocurrency*, termasuk serangan siber canggih yang menargetkan aset digital, menambah tekanan terhadap tim SOC untuk segera meningkatkan kapasitas dan kapabilitas mereka.

Ancaman terhadap integritas data, ketersediaan layanan keuangan, dan privasi pengguna yang semakin meningkat, mendorong perusahaan XYZ untuk memperkuat sistem keamanan mereka. Salah satu pendekatan krusial dalam menjaga keamanan perusahaan adalah melalui pembentukan dan pengelolaan tim SOC. tim SOC memainkan peran vital dalam mendeteksi, menanggapi, dan mencegah serangan keamanan siber yang dapat merugikan perusahaan. Namun, perancangan yang efektif dari Tim SOC masih menjadi tantangan utama. Dalam konteks ini, penting untuk mengembangkan model perancangan tim SOC yang efektif dan dapat diimplementasikan di perusahaan XYZ. Model perancangan ini harus mempertimbangkan berbagai faktor, termasuk struktur organisasi, teknologi yang digunakan, proses operasional, dan sumber daya manusia. Tujuannya adalah untuk membangun tim SOC yang tidak hanya mampu merespons insiden siber dengan cepat dan efisien, tetapi juga proaktif dalam mendeteksi dan mencegah ancaman sebelum berdampak pada operasi bisnis.

Atas dasar ini, pimpinan perusahaan meminta dilakukan sebuah penelitian untuk mengembangkan model perancangan tim SOC yang dapat diimplementasikan secara efektif di perusahaan XYZ. Penelitian ini diharapkan dapat memberikan panduan praktis dalam membentuk dan mengelola tim SOC yang mampu merespons ancaman siber secara proaktif, sekaligus meningkatkan kesiapan dan ketangguhan operasional perusahaan dalam menghadapi tantangan keamanan yang semakin kompleks. Melalui studi kasus pada perusahaan XYZ, penelitian ini akan mengidentifikasi faktor-faktor kunci yang mempengaruhi efektivitas tim SOC dan mengusulkan *best practices* dalam perancangan dan implementasi tim SOC. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan panduan praktis bagi perusahaan XYZ dalam membentuk dan mengelola tim SOC yang efektif dan efisien.

2. TINJAUAN PUSTAKA

2.1. Perusahaan Finansial

Perusahaan sektor finansial, dalam lanskap ekonomi modern, menjadi tulang punggung yang menggerakkan aktivitas keuangan dan ekonomi secara keseluruhan (Rizal et al., 2019). Mereka tidak hanya menjadi garda terdepan dalam mengelola keuangan, tetapi juga berfungsi sebagai penjaga integritas pasar dan pengelola risiko secara keseluruhan. Secara umum, perusahaan sektor finansial meliputi institusi-institusi seperti bank, lembaga asuransi, perusahaan investasi, dana pensiun, dan entitas keuangan lainnya yang berperan dalam perantaraan keuangan, pengelolaan risiko, dan penyediaan layanan finansial. Penting untuk dicatat bahwa perusahaan sektor finansial tidak beroperasi secara independen. Mereka terhubung dalam jaringan global yang kompleks, baik melalui kemitraan bisnis, transaksi lintas negara, maupun investasi di pasar global (Syaifullah, 2018). Oleh karena itu, perubahan dalam satu bagian dari ekosistem keuangan global sering kali memiliki dampak yang merambat dan kompleks di seluruh industri.

2.2. *Security Operation Center* (SOC)

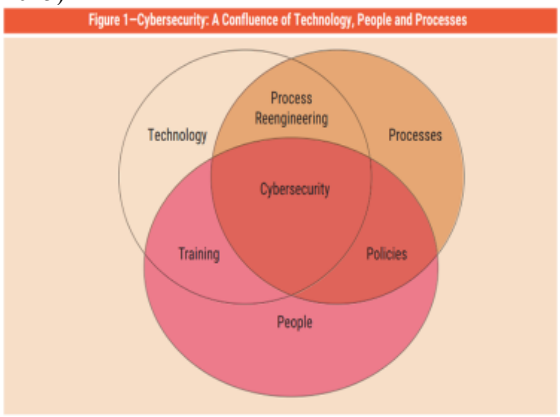
Security Operations Center (SOC) adalah pusat operasi keamanan yang bertugas untuk memantau, mendeteksi, dan merespons insiden keamanan siber dalam suatu organisasi. SOC berfungsi sebagai tim yang terdiri dari para spesialis keamanan siber yang bertanggung jawab untuk menjaga kerahasiaan, integritas, dan ketersediaan sistem dan data organisasi (Knerler et al., 2022).

2.3. *Cryptocurrency Exchange*

Bursa perdagangan mata uang *crypto*, atau *cryptocurrency exchange*, merupakan platform di mana pengguna *cryptocurrency* dapat melakukan jual-beli dan berinteraksi secara langsung (Rahayu, Dwi, 2022). Terdapat dua jenis *cryptocurrency exchange*, yaitu *decentralized exchange* dan *centralized exchange*. Perbedaannya terletak pada pengelolaan dan otoritas dalam operasionalnya. *Decentralized exchange* tidak dijalankan oleh entitas atau perusahaan tertentu, melainkan secara eksklusif oleh perangkat lunak. Ini membuatnya sulit diatur oleh pihak eksternal seperti pemerintah. Sebaliknya, *centralized exchange* dioperasikan oleh entitas atau perusahaan yang mengontrol seluruh proses perdagangan, bergantung pada infrastruktur pribadi untuk mencocokkan penawaran dan permintaan di server mereka sendiri.

2.4 *People, Process and Technology* (PPT) *Framework*

People, Process, and Technology (PPT) Framework adalah pendekatan yang komprehensif untuk mengoptimalkan operasi dan proses bisnis dalam organisasi. Kerangka ini menekankan pentingnya keseimbangan antara elemen manusia (*people*), proses (*process*), dan teknologi (*technology*) dalam mencapai tujuan organisasi dan meningkatkan kinerja keseluruhan (Prodan et al., 2015).



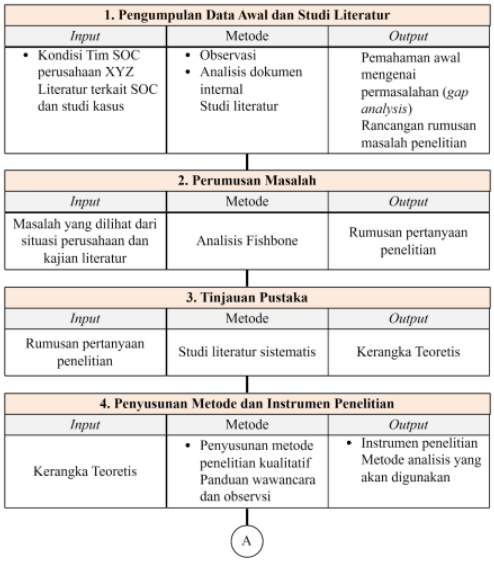
Gambar 1 *People, Process, Technology Framework*

3. METODOLOGI PENELITIAN

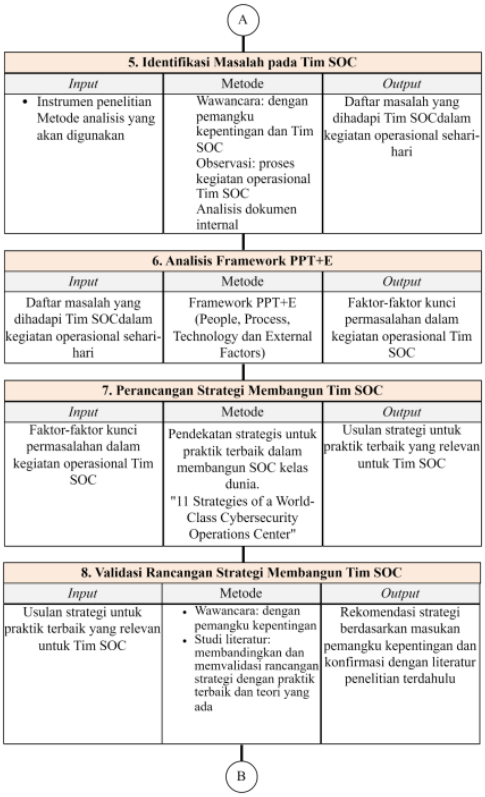
Jenis penelitian yang digunakan adalah *Applied Research* dengan mengadopsi pendekatan kualitatif deskriptif, Pendekatan kualitatif memungkinkan peneliti untuk menggunakan dirinya sebagai instrumen utama dalam mengumpulkan data yang melibatkan pemahaman yang mendalam terhadap faktor-faktor yang mempengaruhi keberhasilan SOC (Alhamid & Budur, 2019). Dalam konteks ini, metode deskriptif, menjadi landasan penelitian yang memandu eksplorasi mendalam terhadap situasi sosial yang terkait dengan keberhasilan SOC secara komprehensif dan terperinci. Penelitian ini menggunakan metode studi kasus (*case study*) untuk menggali secara mendalam dan mendetail mengenai permasalahan yang dihadapi oleh tim SOC di perusahaan XYZ. Dalam penelitian ini, data yang diperoleh melalui wawancara, observasi, dan analisis dokumen dianalisis menggunakan metode analisis tematik. Dalam penelitian ini, wawancara

dilakukan dengan beberapa narasumber, *seperti Head of Security, Lead of SOC, SOC Engineer, Security Engineer*, dan *SOC Analyst*. Penelitian ini dilakukan di perusahaan XYZ.

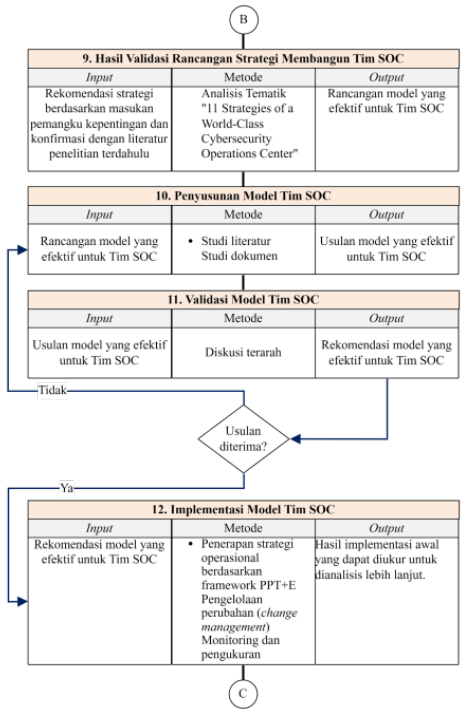
Kerangka teoretis yang digunakan disesuaikan untuk memenuhi kebutuhan strategis SOC di sektor finansial dan ekosistem *cryptocurrency*. Berikut penjabaran alur penelitian pada penelitian ini:



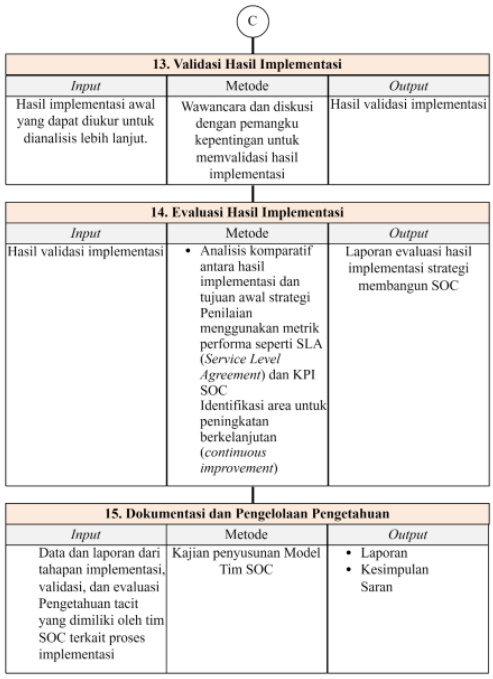
Gambar 2 Alur Penelitian



Gambar 3 Alur Penelitian (Lanjutan)



Gambar 4 Alur Penelitian (Lanjutan)



Gambar 5 Alur Penelitian (Lanjutan)

4. HASIL DAN PEMBAHASAN

4.1. Hasil Audit Bank Sentral dan ISO/IEC 27035 1:2016

Hasil audit Bank Sentral terkait pengelolaan SOC di perusahaan XYZ dapat dihubungkan dengan prinsip-prinsip yang terdapat dalam buku "11 *Strategies of a World-Class Cybersecurity Operations Center*" untuk memberikan konteks lebih mendalam terkait area-area perbaikan yang diidentifikasi dalam audit. Pentingnya SOC sebagai

pusat keamanan informasi telah menjadi fokus dalam tata kelola TI modern. Menurut standar ISO/IEC 27035-1:2016, SOC harus diatur secara jelas dan konsisten, termasuk dalam hal pembentukan tim tanggap insiden (IRT), pelatihan, dan definisi peran.

Pada perusahaan XYZ, kekurangan pemantauan dan peringatan yang memadai mencerminkan adanya kebutuhan untuk pemantauan sistem di mana alat pemantauan yang ada belum cukup mendukung peringatan secara *real-time* dan tidak mencakup seluruh sistem kritis, seperti VPN dan basis data. ISO/IEC 27035-1:2016 menegaskan pentingnya sistem pemantauan dan peringatan yang efektif untuk deteksi tepat waktu kejadian keamanan.

4.2. Roadmap Pengembangan SOC ke Depan

1. Tahap Penguatan Fondasi (1-2 Tahun):
   a. Melakukan rekrutmen tambahan untuk memperkuat tim SOC, serta memberikan pelatihan menyeluruh bagi anggota tim untuk mengatasi kekurangan sumber daya manusia yang ada. Pelatihan ini akan mencakup pembaruan keterampilan dan pengetahuan yang relevan dengan teknologi terkini serta pemahaman mendalam mengenai ancaman yang sedang berkembang.
   b. Pengembangan Kapabilitas Deteksi Ancaman: Mengimplementasikan teknologi canggih seperti Data *Loss Prevention* (DLP), *email gateway*, dan alat pemantauan lainnya.
   c. Menyusun *Standard Operating Procedure* (SOP) dan dokumentasi formal untuk Incident *Security Response Team* (ISIRT). Dokumen ini harus lengkap dan terperinci, guna memastikan konsistensi dalam proses penanganan insiden serta meningkatkan efisiensi tim dalam menghadapi berbagai macam situasi.
   d. Menciptakan budaya kolaborasi yang solid antar departemen sebagai langkah yang krusial dalam pengelolaan keamanan informasi. Hal ini bertujuan untuk membangun integrasi yang lebih baik, sehingga semua pihak terkait dapat berkontribusi dan berkoordinasi secara efektif dalam merespons serta mengelola risiko keamanan.
2. Tahap Peningkatan Proaktif (2-4 Tahun)
   a. Perekrutan spesialis seperti *threat intelligence analyst* dan *threat hunter* untuk memperkuat tim SOC. Keberadaan spesialis ini akan meningkatkan kemampuan dalam mendeteksi, menganalisis, dan memitigasi ancaman dengan lebih efisien.
   b. Pengembangan *Platform threat intelligence* dengan sistem SIEM (*Security Information and Event Management*) dan solusi keamanan lainnya. Integrasi ini bertujuan untuk memaksimalkan deteksi ancaman dan memberikan informasi yang lebih akurat dalam pengambilan keputusan.
   c. SOC akan menyelenggarakan *tabletop exercises* dan *breach-and-attack simulations* secara berkala. Kegiatan ini bertujuan untuk menguji dan menyempurnakan kesiapan tim dalam merespons insiden siber, serta untuk meningkatkan keterampilan dan koordinasi antara anggota tim.
   d. Pengembangan proses *threat hunting* sebagai langkah proaktif dalam menghadapi potensi ancaman. Ini mencakup pemantauan dan analisis secara berkesinambungan untuk menemukan indikasi ancaman sebelum mereka dapat berakibat merugikan.
3. Tahap Transformasi Lanjutan (4-6 Tahun):
   a. Peningkatan Kapasitas Teknologi Berbasis AI dan *Machine Learning*: Mengintegrasikan teknologi kecerdasan buatan untuk mendukung analisis ancaman yang lebih kompleks dan otomatisasi dalam pemantauan serta respons insiden.
   b. Implementasi Arsitektur SOC Masa Depan: Mengadopsi model SOC berbasis cloud untuk mendukung skalabilitas, fleksibilitas, dan efektivitas biaya, dengan tetap menjaga kepatuhan terhadap regulasi lokal dan internasional.
   c. Penguatan Ketahanan Operasional: Menambahkan redundansi dalam infrastruktur SOC untuk memastikan kontinuitas operasional, termasuk disaster recovery dan failover systems.
   d. Ekspansi Fungsional SOC: Mengembangkan kapabilitas SOC untuk mencakup area seperti monitoring dark web, analisis kejahatan siber berbasis blockchain, dan perlindungan infrastruktur kritis lainnya.
   e. Evaluasi dan Optimalisasi Berkelanjutan: Untuk menjaga keunggulan kompetitif dan efektivitas operasional, menerapkan metrik kinerja SOC secara berkala. Melalui evaluasi mendalam terhadap efektivitas dan efisiensi operasi, melakukan iterasi dan perbaikan proses secara kontinu. Ini memastikan adaptasi terhadap dinamika ancaman yang selalu berubah dan kebutuhan bisnis yang berkembang.

4.3. Strategi Membangun Tim SOC Kelas Dunia

11 strategi utama yang digunakan untuk membangun SOC kelas dunia berdasarkan pendekatan "11 *Strategies of a World-Class Cybersecurity Operations Center*". Strategi-strategi ini dirancang untuk membantu perusahaan XYZ menghadapi tantangan keamanan siber yang semakin kompleks dan mendukung pengembangan SOC yang tangguh, efektif, dan berkelanjutan. Setiap strategi berfokus pada aspek-aspek penting yang berkaitan dengan sumber daya manusia, proses, teknologi, dan faktor eksternal yang memengaruhi keberhasilan operasional SOC. Tabel 1 merupakan deskripsi lebih terperinci dari 11 strategi utama yang digunakan.

Tabel 1 Strategi Membangun Tim SOC Kelas Dunia

Nama Strategi	Penjelasan	Poin Utama	Tantangan	Manfaat Potensial
Strategi 1: Ketahui Apa yang Dilindungi dan Mengapa	Mengembangkan kesadaran situasional tentang misi, regulasi, dan lingkungan data yang perlu dilindungi.	Pemahaman tentang sistem kritis dan ancaman yang relevan.	Kebutuhan sumber daya untuk pemantauan berkelanjutan.	Peningkatan prioritas tindakan SOC berdasarkan konteks risiko.
Strategi 2: Berikan Wewenang kepada SOC untuk Menjalankan Tugasnya	Memberikan wewenang formal kepada SOC melalui piagam organisasi, menyesuaikannya dengan tujuan perusahaan.	Penyelarasan peran SOC dan peran formal dalam organisasi.	Risiko terbatasnya wewenang yang dapat memengaruhi respons insiden.	Kemampuan respons insiden yang lebih baik dan kejelasan peran dalam insiden kritis.
Strategi 3: Bangun Struktur SOC Sesuai Kebutuhan	Merancang struktur SOC berdasarkan ukuran organisasi, kebutuhan layanan, dan fungsi SOC yang diinginkan.	Struktur yang fleksibel untuk berbagai skenario keamanan.	Keseimbangan kebutuhan staf dengan biaya operasional.	Struktur SOC yang selaras dengan tujuan spesifik organisasi.
Strategi 4: Rekrut dan Kembangkan Staf Berkualitas	Memfokuskan pada perekrutan profesional terampil serta menciptakan lingkungan kerja yang mendukung pengembangan.	Pelatihan, retensi, dan pengembangan karier.	Tingginya tingkat *turnover* dalam peran keamanan siber.	Tenaga kerja SOC yang terampil, termotivasi, dan stabil.
Strategi 5: Prioritaskan Respons Insiden	Menyusun kategori insiden, langkah-langkah respons, dan jalur eskalasi untuk penanganan yang konsisten.	Proses respons yang terstandar dan jalur eskalasi yang jelas.	Menjaga respons insiden yang efektif dalam skala besar.	Respons yang konsisten dan cepat terhadap insiden, mengurangi dampak pelanggaran.
Strategi 6: Kenali Lawan dengan Intelijen Ancaman Siber (CTI)	Menggunakan Intelijen Ancaman Siber untuk memahami taktik, teknik, dan prosedur lawan.	Strategi pertahanan yang berbasis informasi ancaman.	Tantangan dalam integrasi dan analisis CTI.	Visibilitas ancaman yang lebih besar dan fokus pada pertahanan proaktif.
Strategi 7: Pilih dan Kumpulkan Data yang Tepat	Mengutamakan pengumpulan data yang bernilai dari jaringan, sistem *host*, dan cloud untuk meningkatkan efektivitas SOC.	Pengumpulan data penting, manajemen *log*.	Pengelolaan volume data dan memastikan pengumpulan data yang relevan.	Pemantauan aset yang komprehensif dan efisien.
Strategi 8: Manfaatkan Alat untuk Mendukung Alur Kerja	Memanfaatkan SIEM, SOAR, UEBA, dan alat lainnya untuk menyederhanakan proses dan alur kerja SOC.	Integrasi alat, alur kerja yang lebih baik.	Biaya dan kompleksitas dalam mengelola berbagai alat.	Peningkatan produktivitas analis dan waktu respons insiden yang lebih cepat.
Strategi 9: Komunikasi, Kolaborasi, dan Berbagi	Meningkatkan komunikasi dalam SOC, dengan pemangku kepentingan, dan komunitas siber yang lebih luas.	Pembaruan rutin, kolaborasi dengan SOC lainnya.	Memastikan keamanan dan kontrol dalam berbagi informasi.	Kemitraan yang lebih kuat dan akses ke wawasan ancaman siber yang lebih luas.
Strategi 10: Ukur untuk Meningkatkan Kinerja	Mendefinisikan KPI dan metrik lainnya untuk mengevaluasi proses SOC dan mengidentifikasi area perbaikan.	Keputusan berbasis data, optimasi proses.	Biaya pengumpulan dan analisis data.	Peningkatan SOC yang berkelanjutan dengan hasil yang terukur.
Strategi 11: Perluas Fungsi SOC	Menambah kapabilitas seperti *threat hunting*, *red teaming*, dan analisis *malware* setelah SOC mencapai kematangan dasar.	Pertahanan yang lebih canggih dan kapabilitas yang beragam.	Membutuhkan personel terampil dan sumber daya tambahan.	Posisi pertahanan yang lebih kuat dan kemampuan menghadapi ancaman yang kompleks.

4.4. Ancaman dan Resiko Bisnis Pada *Cryptocurenncy Exchange*

Menurut narasumber PN, seorang *Risk Manager* mengungkapkan bahwa ancaman paling signifikan yang dihadapi oleh *cryptocurrency exchange* adalah pelanggaran data dan pencurian crypto yang dikenal dengan istilah "*crypto heists*". Ancaman ini terutama mengarah pada pencurian atau kehilangan dana nasabah, yang juga mencakup ancaman dari dalam (*insider threat*). Ancaman ini dianggap sangat serius karena dapat menyebabkan kerugian besar dan merusak reputasi perusahaan. Dalam konteks ini, Strategi 5: Prioritaskan Respons Insiden sangat relevan, karena tim SOC harus memiliki prosedur respons yang cepat dan efisien

untuk memitigasi dampak dari pelanggaran data dan pencurian dana, terutama pada lingkungan yang dinamis seperti exchange cryptocurrency.

Selain itu, *downtime* sistem juga merupakan ancaman yang signifikan karena *cryptocurrency exchange* dituntut untuk memiliki ketersediaan yang tinggi. Gangguan layanan atau *downtime* dapat menyebabkan hilangnya kepercayaan dari pengguna dan merugikan secara finansial. Volatilitas pasar *crypto* dan *crash* pasar juga memberikan dampak besar pada bisnis, yang bahkan dapat menyebabkan kebangkrutan (*insolvency*).

PN juga menjelaskan bahwa ancaman yang dihadapi oleh cryptocurrency exchange tidak jauh berbeda dengan sektor finansial lainnya, namun ancaman tersebut sering kali lebih intensif. Misalnya, serangan peretasan dan pencucian uang di *cryptocurrency exchange* cenderung lebih parah karena kurangnya regulasi yang ketat dan sifat anonim dari transaksi *cryptocurrency*. Tantangan regulasi merupakan ancaman yang signifikan bagi pertumbuhan bisnis *cryptocurrency exchange*. Pemerintah di berbagai negara memiliki aturan yang berbeda-beda yang dapat membatasi ruang gerak perusahaan dalam berekspansi dan beroperasi. Tantangan regulasi ini sejalan dengan Strategi 1: Ketahui Apa yang Dilindungi dan Mengapa dan Strategi 6: Kenali Lawan dengan Intelijen Ancaman Siber (CTI), di mana memahami regulasi dan pola ancaman yang berbeda di berbagai yurisdiksi dapat membantu perusahaan menyesuaikan strategi pertahanan mereka.

Dalam menghadapi tantangan ini, PN menyebutkan bahwa kompleksitas infrastruktur teknologi dan perubahan yang cepat dalam lingkungan crypto membuat sulit untuk menilai tingkat risiko dari ancaman yang ada dan menentukan tindakan mitigasi yang tepat. Kesiapan regulasi dan kepatuhan terhadap berbagai aturan juga menjadi beban, terutama bagi *startup* yang harus beradaptasi dengan teknologi dan proses baru dengan anggaran terbatas. Bahkan untuk institusi yang lebih matang, mematuhi berbagai regulasi dan audit bisa sangat membebani tim kepatuhan. Strategi 1 : Ketahui Apa yang Dilindungi dan Mengapa dan Strategi 7: Pilih dan Kumpulkan Data yang Tepat sangat penting dalam hal ini, karena dengan mengumpulkan data yang relevan dan mengetahui aset apa saja yang perlu dilindungi, tim SOC dapat lebih baik dalam mengevaluasi risiko dan mengidentifikasi ancaman yang muncul lebih cepat.

Ancaman yang muncul di masa depan termasuk potensi serangan yang menggunakan kecerdasan buatan (AI) dan *quantum computing*. *Quantum computing*, meskipun masih dalam tahap awal, dapat mematahkan protokol enkripsi saat ini dan mengancam keamanan *blockchain*. Untuk menghadapi ancaman ini, organisasi harus terus memantau perkembangan teknologi dan mempersiapkan adaptasi yang diperlukan.

Balancing antara implementasi langkah-langkah keamanan yang ketat dan mempertahankan pengalaman pengguna yang ramah juga merupakan tantangan. Tim SOC harus menggunakan pendekatan berbasis data dalam mengembangkan fitur produk dan mengutamakan umpan balik dari pengguna dan pemangku kepentingan untuk memastikan bahwa langkah-langkah keamanan tidak mengorbankan kenyamanan pengguna. Melalui pendekatan strategi nomor 3: Bangun Struktur SOC Sesuai Kebutuhan maka tim SOC dapat menyesuaikan dengan kebutuhan organisasi untuk memastikan efektivitas dan efisiensi operasional SOC dan strategi nomor 10: Ukur untuk Meningkatkan Kinerja, memantau metrik kinerja SOC yang relevan dapat membantu dalam menyeimbangkan keamanan dan pengalaman pengguna.

Dari wawancara ini, dapat disimpulkan bahwa ancaman dan risiko yang dihadapi oleh *cryptocurrency exchange* sangat beragam dan memerlukan pendekatan yang holistik dalam mitigasi risiko. Kombinasi antara Strategi 1, 3, 5, 6, dan 7 menjadi langkah yang tepat untuk memecahkan permasalahan ini. Kombinasi antara pemantauan yang aktif, adaptasi terhadap regulasi yang ketat, serta kesiapan menghadapi teknologi baru adalah kunci untuk menjaga keamanan dan stabilitas operasional dalam industri *cryptocurrency*.

4.5. Analisis Keseluruhan

Analisis yang telah dilakukan terhadap kondisi saat ini serta rekomendasi yang diajukan, beberapa permasalahan yang muncul dapat diidentifikasi yang diuraikan sebagai berikut

1. Regulasi dan Tata Kelola TI

   Perusahaan XYZ mengalami ketidaksesuaian dengan regulasi yang mengatur tata kelola TI, seperti ketiadaan keanggotaan direktur dewan non-eksekutif dalam Komite Pengarah TI. Hal ini mengindikasikan bahwa terdapat kekurangan dalam implementasi tata kelola TI yang memadai sesuai dengan persyaratan regulasi yang berlaku. Masalah ini dapat mengarah pada risiko pengawasan dan pengambilan keputusan yang tidak independen dalam pengelolaan keamanan informasi perusahaan.
2. Rencana Manajemen Insiden

   Tidak adanya pengujian yang dilakukan pada rencana manajemen insiden serta kurangnya dokumentasi pembaruan atau ulasan berdasarkan simulasi atau insiden sebenarnya menunjukkan rendahnya kesiapan perusahaan dalam menghadapi insiden keamanan. Ini menimbulkan potensi risiko ketika insiden

terjadi, karena tim mungkin tidak siap untuk merespons dengan efektif dan efisien.

3. Tim Tanggap Insiden (IRT)
   Kekurangan Tim Tanggap Insiden yang secara formal ditetapkan dan peran yang ditugaskan secara *ad hoc* dapat mengakibatkan konflik kepentingan dan inefisiensi dalam menangani insiden keamanan. Hal ini menunjukkan bahwa implementasi struktur organisasi dan proses manajemen insiden tidak sesuai dengan standar yang diharapkan.
4. Program Pelatihan dan Kesadaran
   Pelatihan untuk karyawan baru yang tidak sepenuhnya mencakup aspek-aspek penting manajemen insiden dan ketiadaan pelatihan penyegaran periodik menunjukkan rendahnya investasi dalam pengembangan keterampilan dan kesadaran tentang keamanan informasi. Hal ini dapat mengakibatkan kurangnya pemahaman dan kesiapan karyawan dalam menghadapi ancaman keamanan yang berkembang.
5. Peringatan dan Pemantauan
   Alat pemantauan yang tidak memadai, seperti kekurangan peringatan waktu nyata dan cakupan komprehensif untuk semua sistem kritis, menunjukkan bahwa infrastruktur keamanan informasi perusahaan belum optimal. Kurangnya pemantauan dan peringatan yang efektif dapat mengakibatkan keterlambatan dalam mendeteksi dan merespons ancaman keamanan, meningkatkan risiko keberhasilan serangan terhadap perusahaan.

Hasil analisis tersebut dapat disimpulkan bahwa permasalahan yang muncul lebih bersifat implementasi daripada regulasi. Meskipun regulasi seperti ISO/IEC 27035-1:2016 dan BSP Circular 808 §X176.7 telah mengatur standar dan persyaratan yang diperlukan untuk tata kelola TI dan manajemen keamanan informasi, implementasi yang tepat dari aturan-aturan ini masih belum tercapai sepenuhnya dalam Perusahaan XYZ. Oleh karena itu, perusahaan perlu memperbaiki implementasi tata kelola TI dan memperkuat praktik keamanan informasi mereka untuk memastikan kepatuhan terhadap regulasi serta meningkatkan kesiapan mereka dalam menghadapi ancaman keamanan.

Jika permasalahan yang telah diidentifikasi dalam analisis sebelumnya tidak segera diatasi, perusahaan finansial XYZ akan menghadapi berbagai risiko serius yang dapat mengancam operasional dan reputasinya. Ketidaksesuaian dengan regulasi yang mengatur tata kelola TI, seperti ketiadaan keanggotaan direktur dewan non-eksekutif dalam Komite Pengarah TI, dapat mengakibatkan sanksi dari otoritas regulasi. Ketidakpatuhan terhadap standar seperti ISO/IEC 27035-1:2016 dan BSP Circular 808 §X176.7 tidak hanya mengancam kepatuhan perusahaan, tetapi juga dapat berujung pada denda yang signifikan, pembatasan operasional, atau tindakan hukum lainnya.

Tanpa pengujian dan pembaruan yang memadai terhadap rencana manajemen insiden, perusahaan berisiko mengalami respons yang tidak efektif dan lambat terhadap insiden keamanan. Hal ini dapat memperparah dampak insiden, menyebabkan gangguan operasional yang berkepanjangan, serta menurunkan kepercayaan pelanggan dan mitra bisnis. Selain itu, kekurangan Tim Tanggap Insiden yang secara formal ditetapkan akan mengakibatkan penanganan insiden yang tidak terstruktur dan tidak efisien. Hal ini dapat menyebabkan penanganan insiden yang tidak tepat waktu dan tidak memadai, yang pada akhirnya memperbesar kerusakan yang ditimbulkan oleh insiden keamanan tersebut.

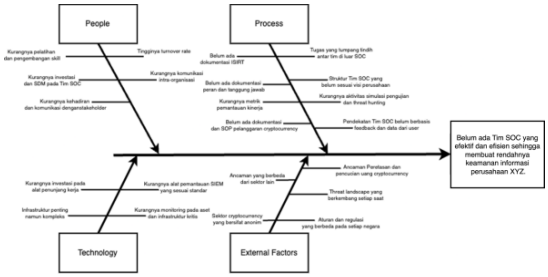
Rendahnya investasi dalam pelatihan dan kesadaran keamanan informasi dapat mengakibatkan kurangnya pemahaman dan kesiapan karyawan dalam menghadapi ancaman keamanan. Karyawan yang tidak terlatih dengan baik cenderung menjadi target yang lebih mudah bagi serangan siber, seperti *phishing*, yang dapat membuka pintu bagi ancaman lebih besar. Alat pemantauan yang tidak memadai, dengan kurangnya peringatan waktu nyata dan cakupan komprehensif untuk semua sistem kritis, meningkatkan risiko keterlambatan dalam mendeteksi ancaman keamanan.

Hal ini memberikan penyerang lebih banyak waktu untuk mengeksploitasi kerentanan dan menyebabkan kerusakan yang lebih besar sebelum respons dapat dilakukan. Kegagalan dalam menjaga keamanan informasi dan ketidak siapan dalam menangani insiden keamanan dapat merusak reputasi perusahaan. Kehilangan data pelanggan atau insiden keamanan besar lainnya akan mengurangi kepercayaan publik dan mitra bisnis terhadap perusahaan, yang pada akhirnya dapat mengurangi pangsa pasar dan pendapatan. semua risiko di atas pada akhirnya akan memiliki dampak finansial yang signifikan. Biaya untuk memulihkan sistem setelah insiden keamanan, denda dari regulator, dan potensi kehilangan bisnis dapat merugikan secara finansial. Selain itu, perusahaan mungkin harus berinvestasi besar-besaran untuk memperbaiki infrastruktur keamanan dan tata kelola TI yang seharusnya telah diimplementasikan sebelumnya.

4.6. Gap Analysis dan Identifikasi Masalah

Berdasarkan temuan dari audit yang dilakukan oleh bank sentral dan wawancara dengan personel SOC, serta sesuai dengan ruang lingkup penelitian ini, berbagai permasalahan dalam pembentukan tim SOC telah berhasil diidentifikasi.

Identifikasi tersebut dilakukan menggunakan metode Diagram Fishbone, yang secara visual menampilkan faktor-faktor penyebab utama serta rincian akar masalah yang memengaruhi efektivitas pembentukan tim SOC, seperti yang ditunjukkan dalam Gambar 6. Tabel 2 memperlihatkan hasil Gap Analysis ysng diperoleh pada perusahaan XYZ.



Gambar 6. Diagram Fishbone Permasalahan Tim SOC Perusahaan X

Tabel 2 Gap Analysis tim SOC Perusahaan XYZ

Harapan	*Gap Analysis*	Ancaman Terhadap Perusahaan
	People	
Anggota SOC memiliki keterampilan yang selalu diperbarui dan relevan dengan ancaman terkini.	Kurangnya pelatihan dan pengembangan *skill* anggota SOC.	Tim tidak siap dalam menangani ancaman kompleks.
Meningkatkan retensi anggota SOC melalui program pelatihan, pengembangan karir, dan insentif.	Tingginya *turnover rate* pada tim SOC.	Hilangnya keahlian dan gangguan operasional.
Memiliki setidaknya 5 anggota SOC dengan keahlian yang relevan.	Kurangnya investasi dan SDM pada tim SOC.	Ketidakmampuan mengatasi ancaman yang berkembang pesat.
Terjalinnya komunikasi yang lebih baik antar divisi untuk mendukung operasional SOC.	Kurangnya komunikasi intra-organisasi.	Koordinasi yang buruk memperlambat penanganan insiden.
Adanya keterlibatan aktif *stakeholder* dalam pengelolaan SOC melalui rapat rutin.	Kurangnya kehadiran dan komunikasi dengan *stakeholder*.	Dukungan strategis untuk SOC menjadi minim.
	Process	
Adopsi pendekatan berbasis data pengguna untuk mendukung keputusan strategis SOC.	Pendekatan belum berbasis data dari pengguna.	Keputusan mitigasi yang tidak tepat sasaran.
Pembagian tugas yang jelas dan terstruktur dengan batasan peran yang didefinisikan.	Tugas yang tumpang tindih dengan Tim di luar SOC.	Efisiensi operasional menurun dan respons insiden terhambat.
Tersedianya dokumen formal yang mendefinisikan peran dan tanggung jawab SOC.	Tidak ada dokumen tertulis terkait peran dan tanggung jawab SOC.	Konflik peran dan kebingungan dalam operasional.
Struktur tim SOC yang mencerminkan visi perusahaan dalam melindungi aset krusial.	Struktur tim SOC belum mencakup aspek perlindungan sesuai visi perusahaan.	Ancaman tidak tertangani secara komprehensif.
Terdapat dokumentasi ISIRT yang terstruktur dan dapat diakses oleh tim terkait.	Belum ada dokumentasi formal tentang ISIRT.	Penanganan insiden tidak terstruktur dan lambat.
Tersedianya SOP formal untuk menangani pelanggaran *cryptocurrency*.	Kurangnya dokumentasi formal dan SOP terhadap pelanggaran *cryptocurrency*	Ketidakpastian dalam menangani pencurian aset *crypto*.
Adanya simulasi dan aktivitas *threat hunting* secara berkala untuk mengantisipasi ancaman.	Kurangnya aktivitas *threat hunting* dan simulasi pengujian sistem	Ancaman tidak terdeteksi hingga berujung pada insiden serius.
Tersedianya metrik standar untuk memantau dan mengevaluasi kinerja SOC secara rutin.	Kurangnya metrik untuk pemantauan kinerja SOC	Sulit mengukur efektivitas dan efisiensi tim SOC.
	Technology	
Implementasi alat SIEM yang sesuai standar industri.	Kurangnya alat pemantauan sesuai standar (SIEM).	Ancaman terlambat terdeteksi, memperbesar dampak serangan.
Adanya anggaran khusus untuk alat-alat yang menunjang operasional SOC.	Kurangnya investasi pada alat penunjang kerja.	Respons terhadap ancaman menjadi lambat dan tidak optimal.
Sistem *monitoring real-time* untuk aset-aset kritis perusahaan.	Kurangnya *monitoring* terhadap aset-aset kritis.	Aset vital tidak terlindungi, meningkatkan risiko pelanggaran data.
Penyederhanaan infrastruktur untuk meningkatkan efisiensi dan kemudahan operasional.	Infrastruktur penting namun kompleks.	Kesalahan konfigurasi membuka celah keamanan.
	External Factors	
Sistem SOC yang mampu mendeteksi dan mencegah ancaman pada *wallet cryptocurrency*.	Ancaman peretasan dan pencucian uang pada sisi *wallet cryptocurrency*.	Risiko reputasi dan kerugian finansial.
Tim SOC memiliki kemampuan adaptasi yang tinggi terhadap perubahan ancaman.	*Threat landscape* yang berkembang setiap saat.	Kesulitan dalam mengantisipasi ancaman baru.

Harapan	*Gap Analysis*	Ancaman Terhadap Perusahaan
Strategi SOC yang disesuaikan dengan karakteristik khusus sektor *cryptocurrency*.	Ancaman yang berbeda dengan sektor lain.	SOC tidak siap menangani ancaman unik di sektor *cryptocurrency*.
Meningkatkan kemampuan analisis anonimitas dengan alat monitoring yang canggih.	Sektor *cryptocurrency* yang bersifat anonim.	Sulitnya melacak aktivitas ilegal seperti pencucian uang.
Penerapan SOC yang fleksibel dan sesuai dengan regulasi lokal di setiap negara operasional.	Aturan dan regulasi berbeda di setiap negara.	Kesalahan kepatuhan hukum dapat berujung pada sanksi atau denda.

4.7. Analisis Masalah dan Solusi

Upaya membangun tim SOC kelas dunia, organisasi sering menghadapi berbagai tantangan yang kompleks, mulai dari keterbatasan sumber daya manusia yang kompeten hingga kurangnya integrasi teknologi yang mendukung. Berdasarkan 11 strategi utama yang dirancang untuk membangun tim SOC yang andal, setiap permasalahan ini dapat diatasi dengan pendekatan yang terstruktur dan inovatif. Strategi-strategi tersebut tidak hanya berfokus pada aspek teknis, tetapi juga pada pengembangan budaya kerja, kolaborasi lintas fungsi, serta pembinaan keterampilan yang berkelanjutan. Subbab ini akan menguraikan permasalahan utama yang dihadapi dalam membangun tim SOC, serta solusi yang diajukan berdasarkan pendekatan strategis tersebut, guna memastikan efektivitas dan ketangguhan tim SOC dalam menghadapi ancaman siber yang terus berkembang. Tabel 3 dijabarkan analisis masalah dan solusi yang dihadapi tim SOC.

Tabel 3 Analisis Masalah dan Solusi

Strategi	Permasalahan	Solusi
Strategi 1: Ketahui Apa yang Dilindungi dan Mengapa	1. Kurangnya pemantauan terhadap sistem kritis (VPN, *Database*, *Wallet*, dll) 2. Ancaman peretasan dan pencucian uang pada sisi wallet cryptocurrency 3. Infrastruktur penting namun kompleks 4. Aturan dan regulasi yang berbeda pada setiap negara terhadap cryptocurrency exchange 5. *Threat landscape* yang berkembang setiap saat, serta ancaman yang berbeda dari sektor-sektor lain 6. Perusahaan global yang mempunya karyawan dari berbagai penjuru belahan dunia	1. Lakukan analisa berdasarkan regulasi,prioritas, kritikalitas aset untuk menentukkan aset mana yang harus dipantau dan dilindungi terlebih dahulu 2. Kumpulkan *log* dari *server* dan *endpoint* karyawan untuk menciptakan visibilitas yang lebih lengkap 3. Buat *rules* pada sistem SIEM untuk mencangkup *threat landscape* yang berkembang pada industri *cryptocurrency*
Strategi 2: Berikan Wewenang kepada SOC untuk Menjalankan Tugasnya	1. Tidak ada dokumen tertulis dari sisi peran dan tanggung jawab SOC 2. Tugas yang tumpang tindih dengan Tim diluar SOC	Tetapkan peran dan tanggung jawab yang jelas di dalam tim SOC melalui piagam resmi atau kebijakan perusahaan, sehingga setiap anggota tahu batas kewenangannya.
Strategi 3: Bangun Struktur SOC Sesuai Kebutuhan	1. Struktur tim SOC belum mampu mencakup semua aspek perlindungan yang sesuai dengan visi dan misi perusahaan 2. Pendekatan belum berbasis data dari pengguna	Rancang struktur tim SOC yang disesuaikan dengan ukuran organisasi, kebutuhan layanan, dan fungsi yang ingin dicapai untuk mendukung kebutuhan internal dan stakeholder.
Strategi 4: Rekrut dan Kembangkan Staf Berkualitas	1. Tingginya *turnover rate* pada tim SOC 2. Kurangnya pelatihan dan pengembangan terhadap *skill* dari anggota tim SOC 3. Kurangnya investasi dan SDM pada tim SOC	Rekrut personel SOC yang berkualitas dan berikan pelatihan berkelanjutan untuk mempertahankan tenaga kerja yang kompeten. Sediakan jalur karier yang menarik untuk mengurangi *turnover*.
Strategi 5: Prioritaskan Respons Insiden	1. Belum ada dokumentasi formal tentang ISIRT 2. Kurangnya *monitoring* terhadap aset-aset kritis 3. Kurangnya dokumentasi formal dan SOP terhadap pelanggaran dan pencurian *cryptocurrency*	Kategorikan insiden berdasarkan tingkat kritikalitas dan gunakan rencana respons yang jelas untuk memastikan insiden yang paling kritis ditangani terlebih dahulu.
Strategi 6: Kenali Lawan dengan Intelijen Ancaman Siber (CTI)	1. Ancaman yang berbeda dengan sektor-sektor lain 2. Sektor *cryptocurrency* yang bersifat anonim 3. Risiko terhadap peretasan dan pencucian *cryptocurrency*	Gunakan intelijen ancaman untuk memahami pola serangan lawan, serta mempersiapkan pertahanan berbasis data yang proaktif tentang ancaman yang sedang berkembang.
Strategi 7: Pilih dan Kumpulkan Data yang Tepat	1. Kurangnya pemantauan terhadap sistem kritis (VPN, *Database*, *Wallet*, dll) 2. Infrastruktur yang kompleks	Identifikasi sumber data yang penting untuk mendeteksi ancaman. Gunakan teknologi untuk mengelola dan memfilter data agar lebih relevan untuk analisis SOC.

Strategi	Permasalahan	Solusi
Strategi 8: Manfaatkan Alat untuk Mendukung Alur Kerja	1. Kurangnya alat pemantauan yang sesuai standar (SIEM) 2. Teknologi keamanan yang kurang memadai 3. Kurangnya investasi pada alat penunjang kerja	Pembelian dan penggunaan alat seperti SIEM, SOAR, atau UEBA untuk mendukung alur kerja SOC, sehingga meningkatkan efisiensi dan otomatisasi proses.
Strategi 9: Komunikasi, Kolaborasi, dan Berbagi	1. Kurangnya kehadiran dan komunikasi dengan *stakeholder* 2. Kurangnya komunikasi intra-organisasi	Libatkan *stakeholder* utama dalam pengambilan keputusan dan lakukan pertemuan lintas tim secara berkala untuk membangun kolaborasi yang efektif.
Strategi 10: Ukur performa untuk Meningkatkan Kinerja	Kurangnya metrik untuk pemantauan kinerja SOC	Tetapkan metrik kinerja utama (KPI) untuk mengevaluasi kinerja SOC secara berkala dan identifikasi area yang perlu ditingkatkan.
Strategi 11: Perluas Fungsi SOC	Kurangnya aktivitas *threat hunting*, *breach* and *attack simulation*, *table top excersise* untuk pengujian sistem *incident response*	Tambahkan fungsi *threat hunting* dan pengujian berbasis skenario seperti *tabletop exercises* untuk meningkatkan kesiapan tim SOC.

4.8. Hasil Penerapan Solusi Berdasarkan 11 Strategi Membangun Tim SOC Kelas Dunia

Penerapan solusi berdasarkan 11 strategi membangun tim SOC kelas dunia memberikan dampak signifikan terhadap peningkatan kapabilitas, efektivitas, dan efisiensi operasional SOC. Strategi-strategi ini mencakup pendekatan komprehensif, mulai dari pengembangan kompetensi personel, implementasi proses kerja yang terstandar, hingga pemanfaatan teknologi terkini yang relevan dengan kebutuhan organisasi. Hasil penerapan solusi ini terlihat dalam beberapa aspek utama, seperti peningkatan kemampuan tim SOC dalam mendeteksi dan merespons ancaman secara proaktif, pengurangan waktu respons terhadap insiden (*mean time to respond*), serta penguatan budaya kerja yang kolaboratif dan berbasis pada pengembangan berkelanjutan. Selain itu, penerapan strategi ini juga membantu organisasi dalam mencapai kepatuhan terhadap regulasi keamanan siber dan memperkuat kepercayaan pemangku kepentingan.

Tabel 4 Hasil Penerapan Solusi

Strategi	Permasalahan	Solusi yang Diajukan	Keadaan Setelah
Strategi 1: Ketahui Apa yang Dilindungi dan Mengapa	1. Kurangnya pemantauan terhadap sistem kritis (VPN, *Database*, *Wallet*, dll) 2. Ancaman peretasan dan pencucian uang pada sisi *wallet cryptocurrency* 3. Infrastruktur penting namun kompleks 4. Aturan dan regulasi yang berbeda pada setiap negara terhadap *cryptocurrency* exchange 5. *Threat landscape* yang berkembang setiap saat, serta ancaman yang berbeda dari sektor-sektor lain 6. Perusahaan global yang mempunya karyawan dari berbagai penjuru belahan dunia	1. Lakukan analisa berdasarkan regulasi,prioritas, kritikalitas aset untuk menentukkan aset mana yang harus dipantau dan dilindungi terlebih dahulu 2. Kumpulkan *log* dari *server* dan *endpoint* karyawan untuk menciptakan visibilitas yang lebih lengkap 3. Buat rules pada sistem SIEM untuk mencangkup threat landscape yang berkembang pada indsutri *cryptocurrency*	1. Pada platform SIEM yang baru diprioritaskan untuk *server-server* lingkungan produksi 2. Pengumpulan *Log* terhadap sistem kritis seperti: production *database*, VPN, Jumpserver *logs*, *hot wallet*, *cold wallet* 3. Pemetaan dan pembuatan skala prioritas terhadap infrastruktur dalam perusahaan 4. Pengumpulan *log endpoint* karyawan untuk dibuatkan sistem *monitoring* dan deteksi 5. Pembuatan *custom rules* pada SIEM untuk mengawasi aset-aset kritis agar sesuai dengan peraturan regulasi dan sertifikasi
Strategi 2: Berikan Wewenang kepada SOC untuk Menjalankan Tugasnya	1. Tidak ada dokumen tertulis dari sisi peran dan tanggung jawab SOC 2. Tugas yang tumpang tindih dengan Tim diluar SOC	Tetapkan peran dan tanggung jawab yang jelas di dalam tim SOC melalui piagam resmi atau kebijakan perusahaan, sehingga setiap anggota tahu batas kewenangannya.	*1.* Pembuatan dokumen struktur organisasi dan roles and *responsibilities* pada platform Confluence yang disetujui oleh *head of security* 2. Pembuatan *channel* koordinasi antar tim internal serta pembagian tanggung jawab dengan tim internal
Strategi 3: Bangun Struktur SOC Sesuai Kebutuhan	1. Struktur tim SOC belum mampu mencakup semua aspek perlindungan yang	Rancang struktur tim SOC yang disesuaikan dengan ukuran organisasi, kebutuhan layanan,	Perencanaan pengembangan struktur SOC dengan penambahan personil hingga 4

Strategi	Permasalahan	Solusi yang Diajukan	Keadaan Setelah
	sesuai dengan visi dan misi perusahaan 2. Pendekatan belum berbasis data dari *feedback* pengguna	dan fungsi yang ingin dicapai untuk mendukung kebutuhan internal dan *stakeholder*.	orang pada 2024 yang berisi 1 *Lead of SOC*, *1 SOC Analyst*, dan *2 SOC Engineer*.
Strategi 4: Rekrut dan Kembangkan Staf Berkualitas	1. Tingginya *turnover* rate pada tim SOC 2. Kurangnya pelatihan dan pengembangan terhadap skill dari anggota tim SOC 3. Kurangnya investasi dan SDM pada tim SOC	Rekrut personel SOC yang berkualitas dan berikan pelatihan berkelanjutan untuk mempertahankan tenaga kerja yang kompeten. Sediakan jalur karier yang menarik untuk mengurangi *turnover*.	1. Rekrutmen tambahan direncanakan untuk Tahun 2025 2. dukungan manajemen terhadap tim SOC dengan memberikan penghargaan atas upaya preventif dan mitigatif, serta memastikan alokasi anggaran dan sumber daya yang memadai untuk operasi SOC yang efektif
Strategi 5: Prioritaskan Respons Insiden	1. Belum ada dokumentasi formal tentang ISIRT 2. Kurangnya *monitoring* terhadap aset-aset kritis 3. Kurangnya dokumentasi formal dan SOP terhadap pelanggaran dan pencurian *cryptocurrency*	Kategorikan insiden berdasarkan tingkat kritikalitas dan gunakan rencana respons yang jelas untuk memastikan insiden yang paling kritis ditangani terlebih dahulu.	1. Pada dokumentasi manajemen insiden terdapat peran dan tanggung jawab yang jelas untuk masing-masing perangkat pada perusahaan. 2. Membuat dokumentasi manajemen insiden/*playbook* pada platform *corporate wiki* yang lengkap dengan *flowchart*, *step-by-step* penanganan insiden, kapan harus melakukan eskalasi, dan proses dokumentasi insiden pada platform *ticketing system* 3. Membuat Channel koordinasi bersama dengan *stakeholder*, *security team*, *tech team* untuk memudahkan koordinasi jika terjadi insiden
Strategi 6: Kenali Lawan dengan Intelijen Ancaman Siber (CTI)	1. Ancaman yang berbeda dengan sektor-sektor lain 2. Sektor *cryptocurrency* yang bersifat anonim 3. Risiko terhadap peretasan dan pencucian *cryptocurrency*	Gunakan intelijen ancaman untuk memahami pola serangan lawan, serta mempersiapkan pertahanan berbasis data yang proaktif tentang ancaman yang sedang berkembang.	1. Pembelian dan penggunaan platform *threat intelligence* baik yang berbayar maupun *open-source intelligence* 2. Penggunaan platform CTI untuk memperkaya sistem monitoring dan deteksi SIEM 3. Penggunaan JIRA sebagai *ticketing platform* 4. Penggunaan ZTNA sebagai akses utama terhadap aplikasi internal dan penghapusan penggunaan VPN *open-source*
Strategi 7: Pilih dan Kumpulkan Data yang Tepat	1. Kurangnya pemantauan terhadap sistem kritis (VPN, *Database*, *Wallet*, dll) 2. Infrastruktur yang kompleks	Identifikasi sumber data yang penting untuk mendeteksi ancaman. Gunakan teknologi untuk mengelola dan memfilter data agar lebih relevan untuk analisis SOC.	1. Melakukan koleksi terhadap data-data yang dainggap penting dan juga berguna untuk analisa tim SOC pada platfrom SIEM dengan menggunakan skala prioritas dan risiko seperti: data *alert* dari EDR, alert dari sistem *Email*, transaksi dari *hot* dan *cold wallet*, *database audit logs*, jumpserver

Strategi	Permasalahan	Solusi yang Diajukan	Keadaan Setelah
			logs, *alert* dari firewall, OS *Logging*, NetFlow, dll
Strategi 8: Manfaatkan Alat untuk Mendukung Alur Kerja	1. Kurangnya alat pemantauan yang sesuai standar (SIEM) 2. Teknologi keamanan yang kurang memadai 3. Kurangnya investasi pada alat penunjang kerja	Pembelian dan penggunaan alat seperti SIEM, SOAR, atau UEBA untuk mendukung alur kerja SOC, sehingga meningkatkan efisiensi dan otomatisasi proses.	1. Pembelian SIEM beserta platform SOAR untuk melakukan otomasi 2. Peningkatan kinerja platform honeypot dengan melakukan *deployment* ke semua *environment server*
Strategi 9: Komunikasi, Kolaborasi, dan Berbagi	1. Kurangnya kehadiran dan komunikasi dengan *stakeholder* 2. Kurangnya komunikasi intra-organisasi	Libatkan *stakeholder* utama dalam pengambilan keputusan dan lakukan pertemuan lintas tim secara berkala untuk membangun kolaborasi yang efektif.	1. Pertemuan berkala antar tim SOC dan *Head of security* serta pertemuan antar *Lead of SOC* dengan direksi setiap minggunya 2. Pembuatan channel komunikasi antar tim SOC dengan tim-tim lain yang terlibat dengan operasional tim SOC
Strategi 10: Ukur performa untuk Meningkatkan Kinerja	kurangnya metrik untuk pemantauan kinerja SOC	Tetapkan metrik kinerja utama (KPI) untuk mengevaluasi kinerja SOC secara berkala dan identifikasi area yang perlu ditingkatkan.	1. Dibuatnya KPI untuk tim SOC untuk tahun 2024 yang dibagi tiap kuartil 2. Pembuatan *dashboard* pada platform SIEM untuk mengukur metriks kinerja SOC seperti waktu respons dan waktu penyelesaian insiden
Strategi 11: Perluas Fungsi SOC	Kurangnya aktivitas *threat hunting*, *breach and attack simulation, table top excersise* untuk pengujian sistem *incident response*	Tambahkan fungsi *threat hunting* dan pengujian berbasis skenario seperti *tabletop exercises* untuk meningkatkan kesiapan tim SOC.	1. *Tabletop exercise* direncanakan untuk tahun 2024 dengan fokus pada pengujian *playbook* insiden. 2. Bekerja sama dengan tim *security engineering* untuk mengadakan *breach and attack simulation* pada kuartil 4 tahun 2024 3. Penggunaan platform honeypot pada lingkungan *server-server* produksi

4.9. Pembahasan

Lead of SOC menekankan bahwa tim SOC telah bekerja keras untuk memenuhi harapan operasional yang telah ditetapkan. Meskipun komunikasi dan kolaborasi di antara anggota tim berjalan dengan baik, tantangan utama yang dihadapi tim adalah kurangnya dukungan infrastruktur dan *endpoint control* yang kuat. Saat ini, pengelolaan infrastruktur dan kontrol *endpoint* masih memerlukan bantuan dari tim lain seperti DevOps dan Corporate IT. Hal ini membuat respons terhadap ancaman yang terkait dengan infrastruktur menjadi kurang optimal.

Dari segi teknologi, *Lead of SOC* mengapresiasi dukungan manajemen yang telah menyediakan SIEM sebagai alat utama untuk *monitoring* dan deteksi. Namun, anggaran yang disediakan untuk mengakomodasi peningkatan kapasitas SIEM belum mencukupi. Tim diharapkan untuk mengonfigurasi dan mengintegrasikan banyak *log*, tetapi tanpa anggaran yang memadai untuk meningkatkan kapasitas *ingestion*, hal ini membatasi efektivitas SIEM dalam menangani jumlah data yang besar.

Evaluasi kinerja tim SOC dilakukan secara berkala, yaitu setiap 4 hingga 6 bulan. Selain itu, *sprint planning* dilakukan setiap minggu untuk memastikan tim tetap berada di jalur yang tepat dalam menyelesaikan tugas-tugas yang telah direncanakan. Dari evaluasi tersebut, ditemukan ahwa kemampuan teknis anggota tim sudah sangat baik, dan komunikasi di dalam tim juga berjalan lancar. Namun, peningkatan proaktivitas dalam menangani ancaman masih diperlukan, terutama dalam hal deteksi dini dan penanganan infrastruktur.

Rekomendasi *Lead of SOC* adalah peningkatan anggaran untuk kapasitas SIEM dan peningkatan koordinasi dengan tim DevOps serta *Corporate IT*. Dengan adanya dukungan lebih dalam hal infrastruktur dan *endpoint control*, tim SOC akan dapat lebih efektif dalam merespons ancaman serta meningkatkan proaktifitas dalam mendeteksi dan mencegah serangan.

Dari sudut pandang *Head of Security* (CISO), performa tim SOC secara keseluruhan dinilai sudah cukup baik dalam mendukung strategi keamanan informasi perusahaan. Tim SOC telah berhasil memberikan visibilitas dan kontrol yang lebih baik terhadap ancaman keamanan, dan investasi yang dilakukan dalam teknologi serta perekrutan personel baru dianggap sesuai dan memberikan dampak positif bagi perusahaan. Meski demikian, CISO menyatakan bahwa ada ruang untuk perbaikan, terutama dalam hal peningkatan pro aktivitas tim dalam menghadapi ancaman siber yang semakin kompleks.

Manajemen juga memberikan dukungan melalui pertemuan mingguan yang diadakan untuk memberikan pembaruan mengenai perkembangan dan tantangan yang dihadapi oleh tim SOC. Laporan rutin dari SOC sudah memenuhi kebutuhan manajemen dalam hal informasi terkait keamanan dan risiko yang sedang dihadapi perusahaan. Hal ini memberikan keyakinan bahwa SOC memiliki kontrol yang lebih baik dan mampu memberikan respon yang tepat terhadap insiden.

Head of Security menyarankan agar fokus di masa depan adalah meningkatkan kemampuan proaktif SOC dalam mengantisipasi ancaman serta meningkatkan kerja sama lintas departemen untuk mengoptimalkan kontrol infrastruktur dan *endpoint*. Harapan ke depannya adalah SOC dapat lebih terintegrasi dengan departemen lain dalam perusahaan, sehingga SOC dapat berfungsi lebih efektif dalam melindungi aset digital dan informasi perusahaan.

Dari wawancara tersebut, dapat disimpulkan bahwa meskipun tim SOC telah menunjukkan performa yang baik dalam beberapa aspek, terutama dalam komunikasi internal dan respons insiden, masih terdapat beberapa tantangan yang harus diatasi. Kurangnya dukungan infrastruktur dan kontrol *endpoint*, serta keterbatasan anggaran untuk peningkatan kapasitas SIEM, menjadi hambatan utama dalam meningkatkan efektivitas tim SOC.

Kedua pemimpin, *baik Lead of SOC* maupun Head of Security, sepakat bahwa kolaborasi dengan tim lain dan peningkatan proaktifitas tim dalam mendeteksi ancaman adalah prioritas yang harus dicapai ke depan. Implementasi dari rekomendasi ini akan sangat membantu tim SOC dalam meningkatkan efisiensinya dan menjaga stabilitas keamanan informasi perusahaan secara lebih menyeluruh.

5. KESIMPULAN DAN SARAN

Hasil penelitian menunjukkan bahwa implementasi strategi ini tidak hanya memberikan panduan praktis, tetapi juga menawarkan pendekatan yang dapat disesuaikan dengan kebutuhan unik perusahaan XYZ, khususnya dalam menghadapi ancaman yang terus berkembang di sektor *cryptocurrency exchange*.

Salah satu kontribusi penting dari penelitian ini adalah identifikasi permasalahan spesifik yang dihadapi oleh Tim SOC di perusahaan XYZ, seperti kurangnya dokumentasi formal ISIRT, tumpang tindih tugas, dan keterbatasan investasi teknologi. Solusi yang diusulkan melalui penelitian ini, seperti penguatan komunikasi intra-organisasi, penerapan teknologi berbasis SIEM dan SOAR, serta penyusunan SOP yang spesifik untuk cryptocurrency, terbukti memberikan dampak langsung terhadap peningkatan efektivitas operasional Tim SOC.

Evaluasi yang dilakukan oleh *Lead of SOC* dan *Head of Security* (CISO) menunjukkan adanya peningkatan signifikan dalam visibilitas ancaman siber, kecepatan respons insiden, serta koordinasi lintas tim. Temuan ini mempertegas bahwa strategi-strategi yang diterapkan tidak hanya relevan secara teoritis, tetapi juga berhasil diterapkan dalam konteks operasional nyata.

Selain itu, penelitian ini menyoroti bahwa keberhasilan SOC sangat bergantung pada dukungan manajemen puncak, tidak hanya dalam alokasi anggaran tetapi juga dalam menyediakan infrastruktur yang memadai dan memastikan sinergi antar divisi. Kendala seperti keterbatasan kapasitas ingestion data dan kurangnya kontrol endpoint dapat diminimalkan dengan kolaborasi lebih erat antara SOC, DevOps, dan tim *Corporate IT*.

Penelitian ini juga menawarkan wawasan baru terkait pengelolaan SOC dalam konteks industri *cryptocurrency* yang memiliki risiko dan dinamika berbeda dari sektor lainnya. Implementasi strategi seperti threat hunting berbasis intelijen siber (CTI) dan pengelolaan ancaman real-time menunjukkan bahwa SOC tidak hanya reaktif tetapi juga proaktif dalam menghadapi ancaman yang berkembang.

Kesimpulannya, penelitian ini memberikan kontribusi otentik dalam merancang Tim SOC yang lebih efektif dan adaptif di perusahaan sektor finansial. Namun, tantangan yang teridentifikasi, seperti keterbatasan anggaran dan perlunya integrasi lintas tim, menunjukkan bahwa dukungan lebih lanjut dari manajemen sangat penting untuk keberlanjutan dan pengoptimalan kinerja SOC. Langkah-langkah peningkatan yang bersifat holistik, termasuk investasi tambahan pada teknologi dan penguatan kolaborasi antar tim, menjadi rekomendasi utama untuk pengembangan lebih lanjut.

5.1. Rekomendasi untuk Penelitian dan Implementasi Lanjutan

Perusahaan disarankan untuk menerapkan 11 Strategi Membangun Tim SOC Kelas Dunia secara menyeluruh, dengan menyesuaikan langkah-langkah implementasinya sesuai dengan kebutuhan spesifik organisasi. Berdasarkan temuan dari penelitian dan hasil wawancara, beberapa saran untuk

meningkatkan kinerja tim SOC di masa mendatang adalah sebagai berikut:

1. Melakukan Pengujian Solusi Lanjutan:
   a. Mengintegrasikan alat otomatisasi yang lebih canggih.
   b. Mengeksplorasi faktor budaya yang memengaruhi kinerja tim SOC.
2. Peningkatan Anggaran untuk SIEM dan Infrastruktur:
   a. Mendukung kapasitas ingestion data yang lebih besar untuk memungkinkan pemantauan lebih banyak log dan deteksi ancaman yang lebih efektif.
   b. Memprioritaskan kontrol infrastruktur dan endpoint untuk meningkatkan deteksi dan mitigasi ancaman.
3. Kolaborasi Lintas Tim yang Lebih Kuat:
   a. Memfasilitasi komunikasi antar departemen, seperti dengan DevOps dan Corporate IT.
   b. Menempatkan perwakilan tim SOC dalam pertemuan lintas departemen.
4. Penguatan Pelatihan dan Pengembangan Personel: Mengadakan pelatihan berkelanjutan dan mempromosikan sertifikasi profesional.
5. Evaluasi Kinerja yang Lebih Mendalam:
   a. Menambahkan indikator kinerja proaktif seperti waktu deteksi ancaman dan jumlah ancaman yang berhasil dicegah sebelum eskalasi.
6. Dukungan Manajemen yang Lebih Fokus:
   a. Menyediakan anggaran fleksibel untuk kebutuhan spesifik SOC.
   b. Memberikan kebebasan kepada tim SOC untuk mengajukan rekomendasi teknologi baru.
7. Peningkatan Proaktifitas dalam Deteksi Ancaman: Berinvestasi dalam alat otomatisasi, AI, dan machine learning untuk menganalisis pola ancaman yang lebih kompleks.

Dengan mengimplementasikan rekomendasi ini, tim SOC diharapkan dapat terus meningkatkan efektivitas operasionalnya, memperkuat postur keamanan informasi perusahaan, dan secara proaktif merespons tantangan ancaman siber yang semakin kompleks.

DAFTAR PUSTAKA

Alhamid, T., & Budur, A. (2019). Resume: Instrumen Pengumpulan Data. *Sekolah Tinggi Agama Islam Negeri (Stain)*, 1–20.

Ariawan, Dudik, P., Sudiarta, Wayan, I., & Sudita, Ketut, I. (2019). Proses Pengajaran Mosaik Di Smk Negeri 1 Sukasada. *Jurnal Pendidikan Seni Rupa Undiksha*, *9*(2), 69–76.

Arifka Sari, A. (2018). Peran Otoritas Jasa Keuangan Dalam Mengawasi Jasa Keuangan Di Indonesia. *Supremasi Jurnal Hukum*, *1*(1).

Avrizal, R., & Haryanto, Y. (2019). Analisis Penerapan Keamanan Sistem Informasi Pada Pt. Axa Mandiri Financial Service Menggunakan Indeks Kami. *Format : Jurnal Ilmiah Teknik Informatika*, *8*(1), 58. Https://Doi.Org/10.22441/Format.2019.V8.I1/008

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Sok: Research Perspectives And Challenges For Bitcoin And Cryptocurrencies. *Proceedings - Ieee Symposium On Security And Privacy*, *2015-July*, 104–121. Https://Doi.Org/10.1109/Sp.2015.14

Braun, V., & Clarke, V. (2006). Using Thematic Analysis In Psychology. *Qualitative Research In Psychology*, *3*(2), 77–101. Https://Doi.Org/10.1191/1478088706qp063oa

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (Senastindo)*, *3*(1), 223–234. Https://Doi.Org/10.54706/Senastindo.V3.2021.141

Conti, M., Sandeep, K. E., Lal, C., & Ruj, S. (2018). A Survey On Security And Privacy Issues Of Bitcoin. *Ieee Communications Surveys And Tutorials*, *20*(4), 3416–3452. Https://Doi.Org/10.1109/Comst.2018.2842460

Creswell, J. W., & Creswell, J. D. (2020). *Research Design: Qualitative, Quantitative, And Mixed Methods Approaches (5th Ed.)*. Sage.

Hägele, S. (2024). Centralized Exchanges Vs. Decentralized Exchanges In Cryptocurrency Markets: A Systematic Literature Review. *Electronic Markets*, *34*(1). Https://Doi.Org/10.1007/S12525-024-00714-2

Hofbauer, J., & Mayer, K. (2024, November). Blue Team Fundamentals: Roles And Tools In A Security Operations Center. *Securware 2024, The Eighteenth International Conference On Emerging Security Information, Systems And Technologies*. Https://Www.Researchgate.Net/Publication/385514927

Knerler, K., Parker, I., & Zimmerman, C. (2022). *11 Strategies Of A World-Class Cybersecurity Operations Center*. The Mitre Corporation.

Kusuma, L. P., & Sutanto, J. E. (2018). Peranan Kerjasama Tim Dan Semangat Kerja Terhadap Kinerja Karyawan Zolid Agung Perkasa. *Performa: Jurnal Manajemen Dan Start-Up Bisnis*, *3*(4), 8.

Majid, M., & Ariffi, K. (2019, October 11). Success Factors For Cyber Security Operation Center

(Soc) Establishment. *Incitest*. Https://Doi.Org/10.4108/Eai.18-7-2019.2287841

Miller, A., Juels, A., Shi, E., Parno, B., & Katz, J. (2014). Permacoin: Repurposing Bitcoin Work For Data Preservation. *Proceedings - Ieee Symposium On Security And Privacy*, 475–490. Https://Doi.Org/10.1109/Sp.2014.37

Mirza. (2021). *Meneropong Arah Sektor Keuangan*.

Oliveira, T., & Fraga Martins, M. (2011). Literature Review Of Information Technology Adoption Models At Firm Level. *The Electronic Journal Information Systems Evaluation*, *14*, 110.

Oosthoek, K., & Doerr, C. (2020). From Hodl To Heist: Analysis Of Cyber Security Threats To Bitcoin Exchanges. *020 Ieee International Conference On Blockchain And Cryptocurrency (Icbc)*, 1–9. Https://Doi.Org/10.1109/Icbc48266.2020.9169412.

Oscar Fanggidae, F., & Akbar Norrahman, R. (2023). Analisis Kualitatif Kebijakan Pengembangan Produk Fintech Dalam Meningkatkan Akses Keuangan Dan Perilaku Konsumen Di Indonesia. *Sanskara Akuntansi Dan Keuangan*, *02*(01), 28–37. Https://Doi.Org/10.58812/Sak.V2i01

Pakpahan, Elvira, F., Chandra, Lionel, R., & Dewa, Ananta, A. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Industri Financial Technology. *Veritas Et Justitia*, *6*(2), 298–323. Https://Doi.Org/10.25123/Vej.3778

Prodan, M., Prodan, A., & Purcarea, A. A. (2015). Three New Dimensions To People, Process, Technology Improvement Model. *Advances In Intelligent Systems And Computing*, *353*, 481–490. Https://Doi.Org/10.1007/978-3-319-16486-1_47

Putri Rizkia Wardhani. (2023). Peran Teknologi Blockchain Dalam Keamanan Dalam Privasi Data. *Jurnal Ilmu Komputer, Ekonomi Dan Manajemen (Jikem)*, *3*(2), 3897–3905.

Rahayu, Dwi, E. (2022). *Transaksi Digital Cryptocurrency Bitcoin Sebagai Investasi Dalam Perspektif Hukum Islam Dan Hukum Positif*.

Rizal, M., Maulina, E., & Kostini, N. (2019). Fintech Sebagai Salah Satu Solusi Pembiayaan Bagi Umkm. *Adbispreneur*, *3*(2), 89. Https://Doi.Org/10.24198/Adbispreneur.V3i2.17836

Ross, R., Winstead, M., & Mcevilley, M. (2022). *Engineering Trustworthy Secure Systems*. Https://Doi.Org/10.6028/Nist.Sp.800-160v1r1

Santoso, Murti, Adi, W., & Nada, Q. N. (2022). Monitoring Threats Menggunakan Huntbox Dengan Metode Mdr (Managed Detection And Response) Pada Security Operation Center (Soc). *Science And Engineering National Seminar 7*, *7*(7).

Sugiyono. (2018a). *Metode Penelitian Kuantitatif, Kualitatif, Dan Rd*. Alfabeta.

Sugiyono. (2018b). *Metode Penelitian Kuantitatif, Kualitatif, Dan R&D – Mpkk*.

Suratkar, S., Shirole, M., & Bhirud, S. (2020, September 28). Cryptocurrency Wallet: A Review. *4th International Conference On Computer, Communication And Signal Processing, Icccsp 2020*. Https://Doi.Org/10.1109/Icccsp49186.2020.9315193

Susanto, E., Dairo, Lende, A., Firjatullah, Akmal, R., & Pratama, Reza, A. (2023). Analisis Keamanan Informasi Pt. Indofood Sukses Makmur, Tbk : Studi Kasus Tentang Peran Objek Vital, Pengamanan File, Dan Pengamanan Cyber. *Jurnal Manajemen Dan Ekonomi Kreatif*, *1*(3), 79–87.

Syaifullah, A. (2018). Analisis Pengaruh Financial Leverage Dan Operating Leverage Terhadap Stock Return. *Inovasi*, *14*(2), 53. Https://Doi.Org/10.29264/Jinv.V14i2.1928

Tornatzky, L. G., & Fleischer, Mitchell. (1990). The Processes Of Technological Innovation. In *D.C. Heath & Company*. Lexington Books. Https://Books.Google.Com/Books/About/The_Processes_Of_Technological_Innovatio.Html?Hl=Id&Id=Eotraaaamaaj

Wiguna, A., Alfianto, E., Cahya Kumala, E., & Giri Putra Maryadi, M. (2024). Problematikadantantangandalamsektor Perbankandankeuangan Di Tahun 2024. *Neraca: Jurnal Ekonomi, Manajemen Dan Akuntansi*, *2*(6), 627–632. Http://Jurnal.Kolibi.Org/Index.Php/Neraca

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain Technology Overview*. Https://Doi.Org/10.6028/Nist.Ir.8202

Yu, C., Yang, W., Xie, F., & He, J. (2022). Technology And Security Analysis Of Cryptocurrency Based On Blockchain. *Complexity*, *2022*. Https://Doi.Org/10.1155/2022/5835457