Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber

Implementation of the NIST Cybersecurity Framework and CIS Controls as Cybersecurity Risk Management

Vicky Mahendra[1], Benfano Soewito[2]
[1,2]Computer Science Department, BINUS Graduate Program – Master of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia
E-mail: [1]vicky.mahendra@binus.ac.id, [2]bsoewito@binus.edu

Abstrak

Menurut laporan dari *Check Point Reasearch*, terjadi peningkatan sebesar 38% dalam serangan siber global pada tahun 2022 bila dibandingkan dengan tahun 2021. Untuk menghadapi serangan siber global ini, maka perlu disiapkan manajemen risiko dalam menghadapi serangan siber tersebut. Saat ini Kementerian Pekerjaan Umum dan Perumahan Rakyat (PUPR) belum memiliki panduan dalam manajemen risiko. Kementerian PUPR dapat memanfaatkan beberapa kerangka kerja keamanan siber yang telah tersedia, seperti kerangka kerja *NIST Cybersecurity* dan kerangka kerja *CIS Controls* yang juga sering disebut *Critical Security Controls* sebagai langkah dalam manajemen risiko keamanan siber. Penelitian ini dilakukan pada salah satu aplikasi yang sedang berjalan pada Kementerian PUPR. Penelitian ini dimulai dengan pengumpulan data, penilaian kondisi saat ini, identifikasi kondisi saat ini, identifikasi kondisi yang diinginkan, analisis kesenjangan, memberikan rekomendasi dan membuat usulan rencana aksi. Hasil penelitian didapatkan bahwa identifikasi kondisi saat ini mendapatkan skor rata-rata 2.77. Kondisi yang diinginkan/dicapai aplikasi didapat skor rata-rata 3.00. Dari hasil tersebut, terdapat kesenjangan sebesar 0.23. Setelah analisis kesenjangan didapatkan 32 rekomendasi dan mengusulkan rencana aksi dengan isu-isu prioritas tinggi dan sedang. Manajemen risiko menggunakan kerangka kerja *NIST Cybersecurity* dan *CIS Controls* terbukti dapat mengukur kematangan keamanan siber pada infrastruktur aplikasi sehingga dapat mengurangi kemungkinan terjadinya serangan siber.

Kata kunci: Kerangka Kerja *NIST Cybersecurity*; Kerangka Kerja *CIS Controls*; Keamanan Siber; Manajemen Risiko

Abstract

According to a report by Check Point Research, global cyberattacks are projected to increase by 38% in 2022 compared to 2021. To combat this global cyber threat, it is necessary to establish risk management protocols. Currently, there are no guidelines on risk management, but the Ministry of PUPR can utilize established cybersecurity frameworks such as NIST Cybersecurity and CIS Controls framework - Critical Security Controls to incorporate cybersecurity risk management. This research was conducted on one of the applications currently running at the Ministry of PUPR, this research began with data collection, assessment of current conditions, identification of current conditions, identification of desired conditions, analysis of gaps, providing recommendations and making proposed action plans. The results of the study found that the current condition identification obtained an average score of 2.77. The conditions desired/achieved by the application obtained an average score of 3.00. from these results, there is a gap of 0.23, after a gap analysis, 32 recommendations are obtained and propose an action plan. Risk management using the NIST Cybersecurity and CIS Controls framework is proven to be able to measure cyber security maturity in application infrastructure to reduce the possibility of cyber attacks.

Keywords: NIST Cybersecurity Framework; CIS Controls Framework; Cybersecurity; Risk Management

1. PENDAHULUAN

Ruang siber merupakan sebuah jaringan komputer yang terdiri dari layanan, sistem komputer, *embedded processors*, *controllers*, dan informasi yang disimpan atau ditransmisikan melalui jaringan tersebut[1]. Perkembangan teknologi internet menawarkan berbagai kemudahan, pengalaman, dan hiburan [2], seperti kemudahan diakses, diproses, serta digunakan secara global dengan lebih mudah [3]. Meskipun begitu, ancaman serangan siber yang makin meningkat setiap tahunnya tidak bisa dilepaskan dari manfaat internet yang semakin luas. Kenaikan jumlah serangan siber dipicu oleh popularitas internet yang terus meningkat. Jika terjadi serangan, dampaknya bisa sangat merugikan seperti mengganggu jalannya bisnis, layanan pelanggan, terjadinya kebocoran data, serta pelanggaran privasi dan undang-undang perlindungan data. Akibat serangan tersebut, waktu dan biaya yang besar juga bisa terbuang[4][5].

Berdasarkan laporan dari *Check Point Research*, serangan siber global meningkat sebesar 38% pada tahun 2022 dibandingkan tahun 2021 [6], dengan 83% organisasi mengalami setidaknya satu pelanggaran data pada tahun tersebut [7]. Dari data nasional, berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), pada tahun 2022 terdapat dugaan insiden siber dengan jumlah total 399 dugaan insiden siber dengan jumlah jenis dugaan insiden tertinggi yaitu pelanggaran data[8], termasuk di dalamnya serangan siber yang menyita perhatian, salah satunya seperti pelanggaran data yang diungkap peretas *Bjorka*. Serangan siber terjadi akibat adanya kelemahan dalam keamanan aplikasi yang dapat dimanfaatkan untuk melakukan tindakan kejahatan[9]. Keamanan menjadi tantangan utama dalam infrastruktur aplikasi karena adanya potensi ancaman dari pihak internal atau eksternal yang bermaksud merusak, mencuri, atau mengubah data pada sistem. Ancaman tersebut dapat berupa virus, malware, serangan peretas, atau kebocoran informasi dari pegawai yang tidak bertanggung jawab. Oleh karena itu, diperlukan sebuah manajemen risiko didunia siber ini. Untuk membangun manajemen risiko, saat ini telah banyak kerangka kerja keamanan siber yang ditawarkan sebagai manajemen risiko seperti *NIST Cybersecurity, ISO 27000, ISA/IEC 62443, GDPR, dan CIS Controls*.

Semua organisasi baik pemerintah maupun swasta perlu memiliki manajemen risiko yang kuat untuk mengurangi kemungkinan terjadinya serangan siber. Kementerian Pekerjaan Umum dan Perumahan Rakyat (PUPR) dalam menjalankan tugas pokok dan fungsi membutuhkan infrastruktur jaringan dan aplikasi yang berfungsi dengan baik, serta memastikan keamanan dari data dan informasi yang dimilikinya. Saat ini Kementerian PUPR belum memiliki kerangka kerja keamanan siber sebagai manajemen risiko dalam melaksanakan tugas-tugas di atas. Agar dapat mengurangi kemungkinan terjadinya serangan siber. Kementerian PUPR dapat memanfaatkan beberapa kerangka kerja keamanan siber yang sudah tersedia, seperti kerangka kerja *NIST Cybersecurity* dan kerangka kerja *CIS Controls*, untuk melindungi aplikasi dan memitigasi risiko serangan siber yang mungkin terjadi. Kementerian PUPR dapat melindungi data dan informasi yang vital dari serangan dan ancaman yang tidak diinginkan dengan menerapkan penanganan risiko keamanan siber yang efektif. Dengan demikian, tugas-tugas yang diemban oleh Kementerian PUPR dapat berjalan dengan lancar dan memberikan pelayanan yang optimal kepada masyarakat.

Referensi peneliti dalam melakukan penelitian ini adalah penelitian pertama yang dilakukan oleh Tim Weil dan San Murugesan dengan judul penelitian "*IT Risk and Resilience—Cybersecurity Response to COVID-19*", dalam penelitiannya menjelaskan saat ini semua orang terkejut bahwa penyebaran virus corona yang cepat dan global, yang dikenal sebagai COVID-19, dan penyakitnya berdampak besar pada hampir semua hal. Setiap orang mengalami krisis kesehatan masyarakat global yang belum pernah terjadi sebelumnya dan tidak dapat diprediksi. Dalam penelitian Weil dan Murugesan mengusulkan solusi penggunaan kerangka kerja *NIST Cybersecurity* sebagai model ringan bagi perusahaan untuk mengatasi ancaman dan serangan siber yang baru yang dihadirkan oleh *gempa* keamanan siber di masa pandemic COVID-19. Kesimpulan dari penelitian bahwa dalam konteks TI, pandemi telah memberikan peluang untuk mengungkap kelemahan dan kerentanan sistem TI, untuk itu diperlukan sebuah standar dan pedoman kerangka kerja keamanan siber sebagai acuan dalam mengatasi ancaman serangan siber

[10]. Penelitian kedua adalah Penelitian yang dilakukan oleh Fatin Hanifah dan rekan-rekan dengan judul penelitian "*Analisa Kerentanan Pada Vulnerable Docker Menggunakan Alienvault dan Docker Bench For Security Dengan Acuan Framework CIS Control*", dalam penelitiannya menguji secara empiris mengenai analisis kerentanan pada *Vulnerable Docker* menggunakan *vulnerability scanner*. Dari 18 kontrol ada 6 kontrol yang diberikan oleh *CIS Controls V8*, bisa digunakan untuk memitigasi risiko yang terjadi pada penelitian ini [11]. Penelitian ketiga adalah Penelitian yang dilakukan oleh Sri Nikhil Gupta Gourisetti dan rekan-rekan dengan judul penelitian "*Demonstration of the Cybersecurity Framework through Real-World Cyber Attack*", dalam penelitiannya menjelaskan kerangka kerja *NIST Cybersecurity* (CSF) yang dikembangkan oleh *National Institute of Standards and Technology Cybersecurity (NIST)*, menyediakan lima fungsi bersamaan dan berkelanjutan untuk Mengidentifikasi, Melindungi, Mendeteksi, Merespons, dan Memulihkan dari ancaman dan kerentanan dunia maya. Solusi yang ditawarkan adalah mengembangkan *webtool CSF*. Hasil penelitian yang dilakukan Nikhil dkk adalah *webtool CSF* menyediakan serangkaian fasilitas gratis, standar berbasis risiko, dan praktik terbaik (*best practice*) untuk membantu pemilik fasilitas dan operator mengelola risiko keamanan siber dengan lebih baik. Kematangan yang diinginkan dari lima domain keamanan siber ditentukan oleh penilaian inti. *webtool CSF* memungkinkan fasilitas untuk menilai kepatuhan *NIST* dengan *CSF* dan mencatat status keamanan [12].

Penelitian keempat adalah penelitian yang dilakukan Mierzwa dan rekan-rekan dengan judul penelitian "*Proposal for the Development and Addition of a Cybersecurity Assessment Section into Technology Involving Global Public Health*", Dalam studi tersebut, Mierzwa dan rekan-rekan mengusulkan untuk mengadopsi kerangka dan pedoman kesehatan masyarakat yang ada, salah satu kerangka kerja yang dibahas dalam penelitian ini adalah *NIST Cybersecurity*. penelitian ini memberikan referensi untuk bertindak bagi peneliti dan praktisi kesehatan masyarakat global untuk memasukkan analisis risiko dan kerentanan ke dalam proyek yang terkait dengan pengembangan dan implementasi teknologi [13]. Penelitian kelima adalah penelitian yang dilakukan oleh Hassanzadeh dan rekan-rekan dengan judul penelitian "*A Review of Cybersecurity Incidents in the Water Sector*", menjelaskan penilaian kritis mereka atas insiden keamanan siber yang diungkapkan, didokumentasikan, dan berbahaya di sektor air dan air limbah (WSS) untuk memberikan tindakan perlindungan terhadap ancaman siber. Solusi yang ditawarkan oleh Hassanzadeh dkk adalah kerangka kerja *Center for Internet Security* (CIS) yang menyusun daftar langkah-langkah keamanan paling berfungsi yang disebut *CIS Controls* yang harus dipertimbangkan oleh setiap organisasi. kerangka kerja *CIS Controls* menawarkan mekanisme dalam keamanan siber, baik berupa mendeteksi, menyangkal, menipu atas serangan siber yang terjadi karena tidak ada mekanisme pertahanan tunggal yang dapat melindungi sektor air dan air limbah dari ancaman serangan siber [14].

Dari 5 (Lima) penelitian di atas, dapat diambil kesimpulan bahwa kerangka kerja *NIST Cybersecurity* dan *CIS Controls* terbukti dapat menjadi praktik terbaik dalam mengukur kematangan keamanan siber pada objek penelitian sehingga tujuan penelitian dapat tercapai. Perbedaan penelitian ini dengan penelitian sebelumnya adalah pada penelitian sebelumnya, masing-masing penelitian menggunakan satu kerangka kerja dalam mengukur kematangan keamanan siber. Sedangkan pada penelitian ini peneliti menggabungkan dua kerangka kerja yaitu kerangka kerja *NIST Cybersecurity* dan *CIS Controls*. Hal ini dilakukan untuk mengukur kematangan keamanan siber secara lebih lengkap dan detail dibandingkan menggunakan satu kerangka kerja.

Peneliti memilih kerangka kerja *NIST Cybersecurity* karena menurut survei keamanan siber *SANS OT/ICS 2019*, kerangka kerja *NIST Cybersecurity* paling banyak diadopsi oleh organisasi di seluruh dunia[15]. Kerangka kerja *NIST Cybersecurity* juga dapat mengoptimalkan waktu dan mengurangi biaya dengan menyediakan kebutuhan langsung untuk perusahaan atau organisasi yang memintanya[16]. Sedangkan peneliti juga memilih kerangka kerja *CIS Controls* karena beberapa konsep *CIS Controls* lebih luas dan lebih detail daripada konsep kerangka kerja *NIST Cybersecurity*[17], sehingga konsep pada *NIST Cybersecurity* tidak bisa diterapkan tanpa *CIS Controls*. Atas alasan tersebut, penelitian ini, peneliti melakukan pemetaan kerangka kerja

CIS Controls ke dalam kerangka kerja *NIST Cybersecurity.* Di samping itu, Kerangka kerja *NIST Cybersecurity* dan kerangka kerja *CIS Controls* juga mengakomodasi semua aspek keamanan, baik teknologi, proses, maupun manusia, di mana aspek-aspek tersebut menjadi landasan penilaian pada penelitian ini. Dengan begitu, diharapkan dapat membantu Kementerian PUPR agar lebih mudah memahami dan menerapkan manajemen risiko agar dapat mengurangi kemungkinan serangan siber yang terjadi dan meminimalkan kerusakan jika terjadi serangan siber.

2. METODE PENELITIAN

2.1 NIST Cybersecurity

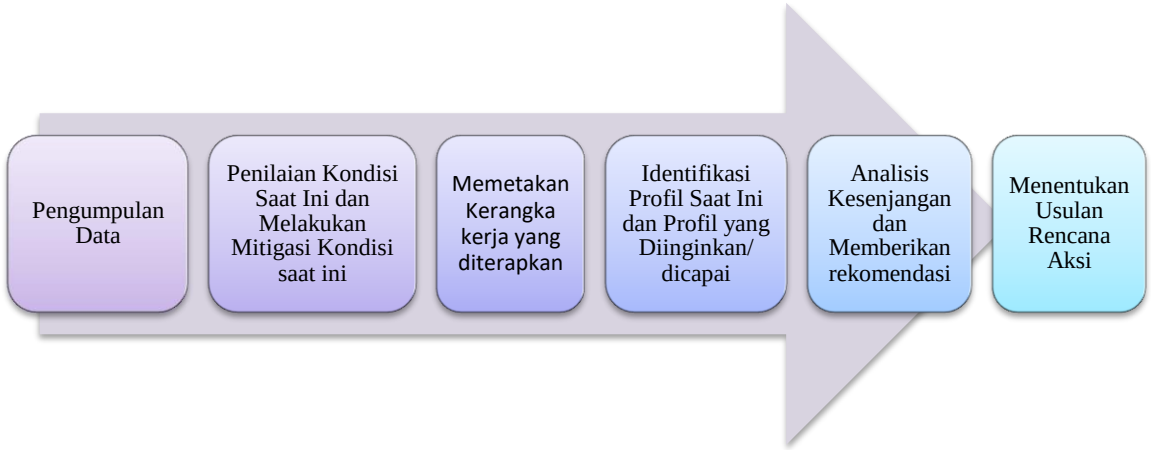
Kerangka kerja *NIST Cybersecurity* digunakan oleh organisasi untuk mengevaluasi sistem dan infrastruktur teknologi informasi yang digunakan untuk menjaga keamanan teknologi dan sistem informasi organiasi dari ancaman siber[18], [19]. Kerangka kerja *NIST Cybersecurity* sudah mencakup standar, metodologi, prosedur, dan pendekatan kebijakan untuk keamanan siber dalam bisnis dan teknologi untuk mencegah ancaman[20]. Elemen inti Kerangka kerja *NIST Cybersecurity* terdiri dari fungsi, kategori, subkategori, dan referensi informasi, di mana lima elemen inti dari Kerangka kerja ini diidentifikasi *sebagai Identify ID, Protect PR, Detect DE, Respond RS, dan Recover RC* [21]. Kerangka kerja *NIST Cybersecurity* pun memainkan peran penting dalam mengidentifikasi potensi ancaman dari berbagai jenis serangan siber[22].

2.2 Critical Security Controls (CIS Controls)

Center for Internet Security, sebuah organisasi nirlaba yang didirikan pada bulan Oktober 2000, membuat kerangka kerja *Critical Security Controls* (*CIS Controls*). Misi organisasi tersebut adalah untuk mengidentifikasi, mengembangkan, memvalidasi, dan mempromosikan praktik pertahanan terbaik dunia siber di seluruh dunia[23]. *CIS Controls* bukan dibuat untuk menggantikan kerangka keamanan siber yang sudah ada seperti *NIST, ISO 27001/27002, PCI DSS[*24], *CIS Controls* dapat membantu organisasi dalam mengambil keputusan keamanan[25]. Ide dasar dari *CIS Controls* adalah bahwa terlalu banyak informasi yang tersedia di Internet tentang perlindungan sistem informasi yang menjadi kontraproduktif, sehingga membuatnya kurang aman[26]. *CIS Controls* terdiri dari 18 kontrol yang masing-masing memiliki sub-kontrol, dan total ada 153 sub-kontrol di seluruh *CIS Controls*[27].

2.3 Tahapan Penelitian

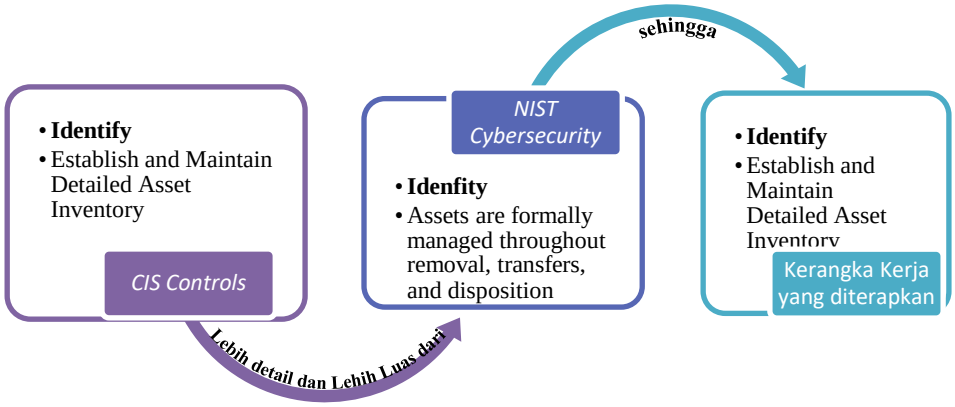
Tahapan penelitian ini meliputi Pengumpulan Data, Penilaian Kondisi Saat Ini, Melakukan Mitigasi, memetakan Kerangka kerja yang diterapkan, Identifikasi Kondisi Saat Ini dan Kondisi yang Diinginkan/ dicapai, Analisis Kesenjangan, Memberikan rekomendasi dan Menentukan Usulan Rencana Aksi.



Gambar 1. Langkah-langkah penelitian

Tahap awal yang dapat dilakukan penelitian ini adalah pengumpulan data kondisi saat ini, agar dapat mengetahui bagaimana keadaan yang terjadi saat ini di Kementerian PUPR. Setelah selesai tahap pengumpulan data, tahap selanjutnya adalah melakukan penilaian kondisi saat ini, di mana berdasarkan data kondisi saat ini, peneliti melakukan penilaian kondisi saat ini. Jika hasil penilaian menunjukkan kerentanan yang tingkat keparahan tinggi, maka tahapan selanjutnya akan dilakukan mitigasi sesuai dengan hasil penilaian.

Kemudian tahap selanjutnya memetakan kerangka kerja yang diterapkan dengan mengidentifikasi kerangka kerja *NIST Cybersecurity* dan *CIS Controls*, kemudian memetakan konsep-konsep dalam Kerangka kerja *CIS Controls* ke dalam kerangka kerja *NIST Cybersecurity*. Hasil pemetaan menjadi Kerangka kerja yang diterapkan dalam penelitian ini dapat dijelaskan pada gambar 2.



Gambar 2. Pemetaan kerangka kerja *CIS Controls* ke dalam *NIST Cybersecurity*

Pada gambar 2 di atas dapat dijelaskan contoh pemetaan kerangka kerja *CIS Controls* ke dalam kerangka kerja *NIST Cybersecurity*, di mana konsep Establish and Maintain Detailed Asset Inventory terdapat pada kerangka kerja *CIS Controls* dengan *security function Identify* memiliki pemetaan hubungan *security function Identify* pada kerangka kerja *NIST Cybersecurity* yaitu *Assets are formally managed throughout removal, transfers, and disposition*. Konsep *Establish and Maintain Detailed Asset Inventory* pada kerangka kerja *CIS Controls* memiliki hubungan implementasi lebih detail dan lebih luas daripada konsep *Assets are formally managed throughout removal, transfers, and disposition* pada kerangka kerja *NIST Cybersecurity*.

Tahapan selanjutnya membangun identifikasi kondisi saat ini. peneliti dalam penelitian ini merujuk pada perusahaan *Intel* yang telah mengadopsi Kerangka Kerja *NIST Cybersecurity* dengan menyesuaikan *tier framework* yang terdiri dari *Tier 1-Partial, Tier 2-Risk Informed, Tier 3-Repeatable*, dan *Tier 4-Adaptive*, yang berfokus pada bidang sumber daya manusia[28]. Tahapan selanjutnya adalah mengidentifikasi kesenjangan dalam persyaratan keamanan siber dan melakukan analisis untuk menemukan cara terbaik untuk mengatasinya. Pada tahap identifikasi kondisi yang diinginkan/dicapai, tujuannya adalah untuk mencapai skor rata-rata kondisi target 3,00, yang sesuai dengan *tier 3 - repeatable* dalam kerangka *tier framework*. Hal ini dilakukan dengan meningkatkan keamanan siber menggunakan skala dan kriteria penilaian tingkat keamanan sistem informasi. Dalam upaya mencapai target tersebut, para pemangku kepentingan terlibat dalam pengambilan keputusan pengembangan aplikasi untuk kondisi yang diinginkan/dicapai.

Setelah mengetahui kesenjangan antara kondisi saat ini dan yang diinginkan/dicapai, dilakukan analisis kesenjangan dilakukan dengan mengevaluasi kondisi saat ini terhadap kondisi yang diinginkan/dicapai, dengan mempertimbangkan rekomendasi yang telah disarankan. Rekomendasi diberikan untuk mencapai kondisi yang diinginkan/dicapai. Pada tahap penetapan usulan rencana aksi, disusunlah rencana aksi yang dapat diambil oleh pimpinan structural Kementerian PUPR untuk mengatasi kesenjangan yang teridentifikasi sebelumnya. Berdasarkan analisis kesenjangan tersebut, rencana aksi dengan 3 jenis isu prioritas yakni tinggi, sedang dan rendah, yang diusulkan mencakup langkah-langkah yang diarahkan untuk mencapai kondisi yang

diinginkan, dengan fokus pada meminimalkan risiko terjadinya serangan siber dan memperkuat praktik keamanan siber yang ada di infrastruktur aplikasi.

3. HASIL DAN PEMBAHASAN

3.1 Pengumpulan Data

Pada tahap ini, peneliti mengumpulkan data tentang aplikasi. Pengumpulan data ini bertujuan untuk mendapatkan informasi mengenai kondisi aplikasi saat ini, oleh karena itu peneliti melakukan observasi, kuesioner dan tinjauan dokumen.

1. Pengamatan : Peneliti mengumpulkan data dengan mengamati atau memantau peristiwa, perilaku, atau fenomena yang terjadi langsung di lapangan. Pengamatan ini dilakukan untuk mendapatkan informasi atau data yang akurat tentang aplikasi yang sedang peneliti pelajari. Pengamatan dapat dilakukan dengan berbagai cara, seperti mengamati dan merekam tingkah laku atau tindakan yang terjadi pada aplikasi, mengamati lingkungan sekitar aplikasi, atau memperhatikan interaksi antara aplikasi dengan penggunanya.
2. Kuesioner : Peneliti melakukan wawancara dengan penanggung jawab aplikasi dan pengguna aplikasi untuk mengumpulkan data dan informasi mengenai keamanan siber aplikasi saat ini, setiap insiden keamanan siber yang mungkin terjadi terhadap aplikasi dalam tiga tahun terakhir, dan kebijakan manajemen risiko yang ada. Dari 63 orang pegawai yang menjadi target pengisian kuesioner, terdapat 33 orang pegawai yang mengisi kuesioner tersebut.
3. Tinjauan dokumen : Peneliti meninjau dokumen-dokumen yang disediakan oleh unit kerja penanggung jawab aplikasi, antara lain Dokumen Alur Proses Bisnis Aplikasi, Dokumen Penggunaan Aplikasi, Dokumen Manajemen Risiko Aplikasi, dokumen keamanan aplikasi dan Peraturan Pemerintah tentang Aplikasi.

Tabel 1**.** Koleksi data hasil

Observasi	Kuesioner	Ulasan Dokumen
Aplikasi belum pernah menjadi sasaran serangan siber hingga penelitian ini dilakukan.	Aplikasi tidak memiliki Manajemen Risiko dan Manajemen setelah insiden dalam tempat setelah terjadi serangan siber	Aplikasi belum memiliki dokumen terkait keamanan aplikasi

Tabel 1 menjelaskan bahwa dalam pengamatan peneliti selama penelitian ini, peneliti menemukan bahwa aplikasi tidak pernah diserang oleh serangan siber. Peneliti juga mengumpulkan data berupa kuesioner, didapatkan bahwa pihak pengelola aplikasi menyatakan bahwa hingga penelitian dilakukan, aplikasi belum memiliki manajemen risiko dan manajemen setelah insiden ketika terjadi serangan siber.Peneliti meninjau dokumen yang terkait dengan aplikasi, dan peneliti menemukan bahwa aplikasi belum memiliki dokumen terkait keamanan aplikasi.

3.2 Penilaian Kondisi Saat Ini dan melakukan mitigasi dari hasil penilaian kondisi saat ini

Penilaian kondisi aplikasi saat ini adalah proses evaluasi yang bertujuan untuk mendapatkan pemahaman yang jelas tentang kondisi aplikasi saat ini. Ini dapat melibatkan berbagai aspek seperti fungsionalitas, kinerja, keamanan, dan kegunaan aplikasi. Untuk penelitian ini, peneliti lebih fokus pada aspek keamanan aplikasi. Proses penilaian ini biasanya dilakukan sebagai bagian dari upaya perbaikan atau pengembangan aplikasi, dengan tujuan untuk memperbaiki masalah atau kekurangan yang ada pada aplikasi agar aplikasi dapat berfungsi lebih baik dan memberikan pengalaman yang lebih baik bagi pengguna. Penilaian kondisi aplikasi saat ini dapat dilakukan melalui berbagai teknik, seperti observasi, kuesioner atau pemeriksaan dokumen.

Skala penilaian umum yang digunakan untuk menentukan tingkat keparahan, seperti skala *Common Vulnerability Scoring System* (*CVSS*), yang memiliki tingkat keparahan berdasarkan skor numerik yang diberikan, dibagi menjadi tiga kategori: Rendah, Sedang, dan

Tinggi. Skor 0 hingga 3,9 tergolong Rendah, skor 4,0 hingga 6,9 tergolong Sedang, dan skor 7,0 hingga 10,0 tergolong Tinggi. Peringkat keparahan ini memberikan informasi penting tentang risiko yang ditimbulkan oleh kerentanan yang teridentifikasi. Dengan mengetahui tingkat keparahan, pengelola aplikasi dapat menentukan tindakan yang akan diambil untuk mengatasi kerentanan dan memperkuat keamanan aplikasi.

Pada tabel 2 dapat dijelaskan bahwa kerentanan yang paling banyak ditemukan adalah *SQL injection* dengan tingkat keparahan yang tinggi. sehingga peneliti melakukan mitigasi dari hasil penilaian kondisi saat ini merupakan tindakan untuk mengurangi atau menghilangkan risiko keamanan yang terdapat pada aplikasi selama proses penilaian. Hal ini dilakukan dengan mengambil tindakan korektif terhadap masalah keamanan yang ditemukan dan mengimplementasikan solusi keamanan yang sesuai untuk mencegah terjadinya masalah serupa di masa mendatang.

Setelah peneliti mengidentifikasi jenis serangan siber yang sangat kritis yang adalah *SQL Injection*. Untuk mengurangi jenis serangan siber ini, peneliti menerapkan strategi untuk menambal kode sumber aplikasi untuk mengatasi kerentanan *SQL Injection* [29]. Tabel 2 menunjukkan bahwa setelah melakukan tindakan mitigasi, sudah tidak ditemukan tingkat keparahan yang tinggi.

Tabel 2. Daftar kerentanan dari hasil penilaian kondisi saat ini dan hasil melakukan mitigasi

Nama	**Hasil Penilaian kondisi saat ini**	**Hasil melakukan mitigasi**
	Tingkat Keparahan	**Tingkat Keparahan**
SQL injection	Tinggi	Tidak ditemukan
Application error messages	Sedang	Sedang
Directory listings	Sedang	Sedang

3.3 Memetakan kerangka kerja yang diterapkan

Setelah dilakukan pengumpulan data, sesuai tabel 3, dilakukan pemetaan kerangka kerja *CIS Controls* ke dalam kerangka kerja *NIST Cybersecurity*. Konsep dalam kerangka kerja *CIS Controls* memiliki pengertian yang lebih detail dan lebih luas dibandingkan dengan konsep dalam kerangka kerja *NIST Cybersecurity*.

Tabel 3. Pemetaan kerangka kerja

Security Function	**Jumlah Konsep dalam Kerangka Kerja yang diterapkan**	
	NIST Cybersecurity	***CIS Controls***
Identify	23	4
Protect	28	10
Detect	16	1
Respond	12	3
Recover	5	0
Total	**84**	**18**
Total Konsep	**102**	

Dari tabel 3 dapat dijelaskan, salah satu *security function* adalah *identify*, di mana memiliki 27 Konsep dalam kerangka kerja yang terdiri dari 24 konsep dari kerangka kerja *NIST Cybersecurity* dan 4 Konsep dari kerangka kerja *CIS Controls* karena memiliki konsep yang lebih detail dan lebih luas dari kerangka kerja *NIST Cybersecurity* seperti pada penjelasan di atas.

3.4 Identifikasi Kondisi Saat Ini dan kondisi yang diinginkan/dicapai

Setelah pemetaan dilakukan, maka dilakukan identifikasi kondisi kondisi saat ini. Ini merupakan sebuah proses yang berfungsi untuk menentukan tingkat keamanan dan kondisi keamanan pada sistem atau aplikasi yang sedang diteliti. Tingkat keamanan mencakup berbagai aspek seperti data, jaringan, dan aplikasi, sedangkan kondisi keamanan mencakup penggunaan fitur keamanan tertentu dalam aplikasi yang bersangkutan. Setelah data terkumpul, didapatkan hasil yang sesuai dengan tabel 4, di mana masing-masing *security function* memiliki nilai rata-rata 2,77 yang sesuai dengan *tier 2 – risk informed* dalam *tier framework*.

Tahapan selanjutnya adalah diskusi dengan pengelola aplikasi untuk merumuskan identifikasi kondisi yang diinginkan/dicapai. Sesuai dengan kesepakatan bersama, rata-rata kondisi yang diinginkan/dicapai untuk setiap *security function* dalam kerangka kerja dengan skor rata-rata 3,00, yang sesuai dengan *tier 3 – repeatable* dalam *tier framework*.

Tabel 4. Identifikasi kondisi saat ini dan kondisi yang diinginkan/dicapai

Security Function	**Kondisi saat ini**	**Kondisi yang Diinginkan/Dicapai**
Identify	2.79	3.00
Protect	2.82	3.00
Detect	2.88	3.00
Respond	2.80	3.00
Recover	2.53	3.00
Rata-rata	**2.77**	**3.00**

Dari tabel 4 dapat dijelaskan, salah satu *security function* adalah *identify*, setelah melakukan assessment kondisi saat ini, peneliti melakukan identifikasi Kerangka kerja dengan hasil assessment kondisi saat ini di mana didapatkan kondisi saat ini dari *identify* diperoleh skor rata-rata 2.79, dan skor rata-rata 3.00 untuk kondisi yang diinginkan atau dicapai. Tabel 4 juga menunjukkan bahwa rata-rata level kondisi yang diinginkan/dicapai memang 3,00.

3.5 Analisis kesenjangan dan memberikan rekomendasi

Tabel 5 menjelaskan rata-rata kesenjangan antara kondisi saat ini dengan kondisi yang diinginkan/dicapai adalah 0,23. Tabel 5 juga menjelaskan kategori *security function Identify*, kebijakan, prosedur, dan proses untuk mengelola dan memantau persyaratan peraturan, hukum, risiko, lingkungan, dan organisasi belum mengadopsi keamanan informasi. Perjanjian dengan entitas eksternal dan pihak ketiga juga belum memiliki aspek keamanan informasi. Pada kategori *security function Protect*, Peneliti menekankan bidang sumber daya manusia, karena tidak semua pengguna aplikasi telah mendapatkan pelatihan atau pendidikan keamanan siber, dan ini ditambah dengan fakta bahwa prosedur dan proses untuk mengelola dan memantau peraturan, hukum, dan persyaratan organisasi belum mengadopsi praktik keamanan informasi.

Tabel 5. Rekapitulasi analisis kesenjangan

Security Function	**Rekapitulasi**		**Kesenjangan**
	Kondisi saat ini	**Kondisi yang Diinginkan/ Dicapai**	
Identify	2.79	3	0.21
Protect	2.82	3	0.18
Detect	2.88	3	0.12
Respond	2.80	3	0.20
Recover	2.53	3	0.47
Rata-rata	**2.77**	**3.00**	**0.23**

Dalam kategori *security function Detect*, saat ini tidak ada prosedur untuk memantau kode berbahaya dan kode seluler, sehingga perlu dibuat prosedur untuk memantau jenis kode ini. Dalam kategori *security function Respond*, peneliti juga menemukan bahwa kebijakan, prosedur, dan proses untuk mengelola dan memantau persyaratan peraturan, hukum, risiko, lingkungan, dan organisasi belum mengadopsi keamanan informasi.

Pada kategori *security function Recover*, kesenjangan paling tinggi dibandingkan *security function* lainnya karena kebijakan dan prosedur penanganan insiden dan pemulihan tidak ada dan tidak terdokumentasi. Karena berdasarkan observasi peneliti di mana dari awal aplikasi dibuat hingga saat penelitian ini dilakukan, belum ada serangan siber terhadap aplikasi tersebut, akan tetapi sebaiknya Kementerian PUPR tetap menyiapkan dokumentasi untuk penanganan insiden dan pemulihan insiden. Saat ini, komunikasi dan koordinasi setelah penanganan insiden hanya dilakukan dengan pihak tertentu dan tidak semua insiden dilaporkan kepada pimpinan struktural dan pengguna lainnya.

Selanjutnya peneliti membuat rekomendasi untuk mengatasi kesenjangan antara kondisi saat ini dan kondisi yang diinginkan/dicapai. Tindakan yang direkomendasikan harus

mendapatkan persetujuan pimpinan struktural Kementerian PUPR sebelum diterapkan. Tabel 6 menunjukkan bahwa peneliti telah mengusulkan total 32 rekomendasi di setiap *security function*.

Tabel 6. Jumlah rekomendasi

Security Function	**Jumlah Rekomendasi**
Identify	9
Protect	11
Detect	3
Respond	5
Recover	4
Total	**32**

3.6 Menentukan usulan rencana aksi

Pada tahap akhir penelitian ini, peneliti mengusulkan rencana aksi yang harus diambil oleh Pimpinan Struktural terkait dengan mengatasi kesenjangan yang teridentifikasi yang dijelaskan di atas. Berdasarkan analisis kesenjangan dan rekomendasi di atas, usulan rencana aksi berikut ini perlu dilaksanakan untuk mencapai kondisi yang diinginkan/dicapai. Hal ini dimaksudkan untuk mengurangi risiko terjadinya serangan siber dan memperkuat praktik keamanan siber yang ada di infrastruktur aplikasi. Seseorang yang bertanggung jawab ditugaskan untuk melaksanakan dan mengelola usulan rencana aksi yang telah ditetapkan dan disetujui oleh pimpinan struktural. Prioritas dan penyelesaian target juga ditentukan berdasarkan hasil analisis kesenjangan dan faktor-faktor prioritas lainnya, termasuk sumber daya manusia, untuk memastikan bahwa kesenjangan prioritas tinggi segera di atasi.

Pada tabel 7 dijelaskan bahwa isu-isu prioritas tinggi yang harus diselesaikan oleh Kementerian PUPR paling lambat 6 bulan sejak tanggal laporan rekomendasi, sedangkan isu-isu prioritas sedang harus diselesaikan paling lambat 12 bulan sejak tanggal laporan rekomendasi.

Tabel 7. Ringkasan rencana tindakan yang diusulkan

Security Function	**Prioritas**		
	Tinggi	**Sedang**	**Rendah**
Identify	5	4	0
Protect	4	7	0
Detect	0	3	0
Respond	2	3	0
Recover	3	1	0
Total	**14**	**18**	**0**

4. KESIMPULAN DAN SARAN

Kesimpulan yang dapat peneliti jelaskan pada penelitian ini adalah hasil penilaian kondisi saat ini pada aplikasi ditemukan terdapat kerentanan terhadap serangan siber *SQL Injection* dengan tingkat keparahan tinggi. Dikarenakan ditemukan kerentanan dengan tingkat keparahan tinggi, peneliti telah melakukan mitigasi dengan cara melakukan penambalan pada kode sumber pada aplikasi, sehingga setelah mitigasi, kerentanan tersebut menjadi tidak ditemukan. Selanjutnya berdasarkan pengumpulan data berupa observasi, kuesioner, tinjauan dokumen dan hasil penilaian kondisi saat ini, peneliti melakukan identifikasi kondisi saat ini dengan menerapkan kerangka kerja hasil dari pemetaan kerangka kerja *CIS Controls* ke dalam kerangka kerja *NIST Cybersecurity*, didapat hasil identifikasi kondisi saat ini memiliki skor rata-rata 2,77. di mana terdapat beberapa kekurangan dalam keamanan aplikasi, antara lain belum ada manajemen penanganan insiden, penanganan pemulihan setelah insiden, kebijakan, prosedur yang tidak lengkap, kurangnya dokumentasi dan *log* terkait aktivitas aplikasi, serta kurangnya pemahaman akan pentingnya keamanan data dan informasi di antara seluruh karyawan.

Selanjutnya peneliti melakukan identifikasi kondisi yang ingin dicapai pada aplikasi tersebut, didapatkan skor rata-rata 3,00. Berdasarkan hasil tersebut, terdapat kesenjangan sebesar 0.23 antara kondisi saat ini dan kondisi yang ingin dicapai, sehingga ditahap selanjutnya, peneliti melakukan analisis kesenjangan, di mana terdapat 32 (tiga puluh dua) rekomendasi dari peneliti

perlu dilaksanakan oleh pimpinan struktural Kementerian PUPR dalam bentuk rencana aksi. Usulan rencana aksi yang peneliti usulkan di antara lain dengan membuat kebijakan atau dokumen yang belum ada seperti dokumen manajemen penanganan insiden, dokumen penanganan pemulihan setelah insiden, kebijakan, prosedur yang tidak ada, serta kebijakan mengalokasikan sumber daya manusia dengan peran terkait keamanan siber, dan rutin melakukan pelatihan kesadaran keamanan siber untuk pegawai Kementerian PUPR yang menggunakan aplikasi tersebut. Usulan rencana aksi tersebut dibagi 3 isu prioritas yakni tinggi, sedang dan rendah. di mana isu-isu prioritas tinggi yang harus diselesaikan oleh Kementerian PUPR paling lambat 6 bulan sejak tanggal laporan rekomendasi, sedangkan isu-isu prioritas sedang harus diselesaikan paling lambat 12 bulan sejak tanggal laporan rekomendasi.

Dalam penelitian ini, penerapan kerangka kerja *NIST Cybersecurity* tidak digunakan sendiri dalam manajemen risiko keamanan siber aplikasi karena beberapa konsep dalam Kerangka Kerja *NIST Cybersecurity* kurang lengkap dan kurang detail dalam mengukur risiko keamanan siber aplikasi. Oleh karena itu, dengan memetakan konsep dalam Kerangka Kerja *CIS Controls* ke konsep dalam Kerangka Kerja *NIST Cybersecurity,* dapat mengukur kematangan keamanan siber pada infrastruktur aplikasi, dan pengguna di Kementerian PUPR lebih mudah memahami sekaligus menerapkan manajemen risiko menggunakan kerangka kerja *NIST Cybersecurity* dan kerangka kerja *CIS Controls* sehingga dapat mengurangi kemungkinan serangan siber yang terjadi dan meminimalisir kerusakan jika terjadi serangan siber.

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada Kementerian PUPR yang telah mendukung terlaksananya penelitian ini.

DAFTAR PUSTAKA

[1] A. Refsdal, B. Solhaug, and K. Stølen, "Cyber-risk Management," 2015, pp. 33–47. doi: 10.1007/978-3-319-23570-7_5.

[2] J. Wu, J. Li, and X. Ji, "Security for cyberspace: challenges and opportunities," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1459–1461, Dec. 2018, doi: 10.1631/FITEE.1840000.

[3] Y. Supriyadi and C. W. Hardani, "Information System Risk Scenario Using COBIT 5 for Risk And NIST SP 800-30 Rev. 1 A Case Study," in *2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 2018, pp. 287–291. doi: 10.1109/ICITISEE.2018.8721034.

[4] I. F. Ashari, V. Oktarina, R. G. Sadewo, and S. Damanhuri, "Analysis of Cross Site Request Forgery (CSRF) Attacks on West Lampung Regency Websites Using OWASP ZAP Tools," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 11, no. 2, pp. 276–281, Aug. 2022, doi: 10.32736/sisfokom.v11i2.1393.

[5] M. Falch, H. Olesen, K. E. Skouby, R. Tadayoni, and I. Williams, "Cybersecurity Strategies for SMEs in the Nordic Baltic Region," *Journal of Cyber Security and Mobility*, Jan. 2023, doi: 10.13052/jcsm2245-1439.1161.

[6] Check Point Research, "Check Point Research Reports a 38% Increase in 2022 Global Cyberattack," 2023. Accessed: Mar. 07, 2023. [Online]. Available: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

[7] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," 2023. Accessed: Mar. 07, 2023. [Online]. Available: https://www.ibm.com/reports/data-breach

[8] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia Tahun 2022," 2023.

[9] A. Alexei and A. Alexei, "Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning," *Article in International Journal of Scientific & Technology Research*, vol. 10, pp. 128–133, 2021.

[10] T. Weil and S. Murugesan, "IT Risk and Resilience—Cybersecurity Response to COVID-19," *IT Prof*, vol. 22, no. 3, pp. 4–10, May 2020, doi: 10.1109/MITP.2020.2988330.

[11] F. Hanifah, A. Budiyono, and A. Widjajarto, "Analisa Kerentanan Pada Vulnerable Docker Menggunakan Alienvault Dan Docker Bench For Security Dengan Acuan Framework CIS Control," in *e-Proceeding of Engineering* , 2021, pp. 8880–8885.

[12] S. Nikhil *et al.*, "Demonstration of the Cybersecurity Framework through Real-World Cyber Attack," in *2019 Resilience Week (RWS)*, 2019. doi: 10.1109/RWS47064.2019.8971822.

[13] S. J. Mierzwa, S. RamaRao, J. Ah Yun, and B. G. Jeong, "Proposal for the Development and Addition of a Cybersecurity Assessment Section into Technology Involving Global Public Health," *The The International Journal of Cybersecurity Intelligence and Cybercrime*, vol. 3, no. 2, pp. 48–61, Nov. 2020, doi: 10.52306/03020420BABW2272.

[14] A. Hassanzadeh *et al.*, "A Review of Cybersecurity Incidents in the Water Sector," *ASCE Journal of Environmental Engineering 2020*, Jan. 2020, doi: 10.1061/(ASCE)EE.1943-7870.0001686.

[15] B. Filkins, D. Wylie, and J. Dely, "SANS 2019 State of OT/ICS Cybersecurity Survey," 2019. Accessed: Mar. 16, 2023. [Online]. Available: https://www.sans.org/white-papers/38995/

[16] A. Belalcazar, M. Ron, J. Diaz, and L. Molinari, "Towards a strategic resilience of applications through the NIST cybersecurity framework and the strategic alignment model (SAM)," in *Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017*, Institute of Electrical and Electronics Engineers Inc., Mar. 2018, pp. 181–187. doi: 10.1109/INCISCOS.2017.29.

[17] The Center for Internet Security (CIS), "CIS Critical Security Controls v8 Mapping to NIST CSF," 2021. Accessed: Mar. 01, 2023. [Online]. Available: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf

[18] R. Kwon, T. Ashley, J. Castleberry, P. McKenzie, and S. N. Gupta Gourisetti, "Cyber threat dictionary using MITRE ATTCK matrix and NIST cybersecurity framework mapping," in *2020 Resilience Week, RWS 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020, pp. 106–112. doi: 10.1109/RWS50334.2020.9241271.

[19] G. Kabanda, "A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations," *Asian Journal of Management, Engineering & Computer Sciences (AJMECS)*, vol. 3, no. 4, pp. 17–34, 2018.

[20] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," *J Cybersecur*, vol. 6, no. 1, Jan. 2020, doi: 10.1093/cybsec/tyaa005.

[21] B. Adi. Pratomo, Awaludin. Marwan, Satriyo. Wibowo, M. Thabib. Kariadi, and Siti. Faridah, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Indonesian Translation)," Gaithersburg, MD, Feb. 2022. doi: 10.6028/NIST.CSWP.04162018id.

[22] L. Ajmi, Hadeel, N. Alqahtani, A. Ur Rahman, and M. Mahmud, "A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia," in *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, Institute of Electrical and Electronics Engineers Inc., May 2019. doi: 10.1109/CAIS.2019.8769470.

[23] Center for Internet Security (Inc), "CIS Critical Security Controls® CIS Critical Security Controls," 2021. [Online]. Available: www.cisecurity.org/controls/

[24] D. P. Prastika, J. Triyono, and U. Lestari, "Audit dan Implementasi CIS Benchmark Pada Sistem Operasi Linux Debian Server (Studi Kasus: Server Laboratorium Jaringan Dan Komputer 6, Institut Sains & Teknologi Akprind Yogyakarta)," *Jurnal JARKOM* , vol. 6, no. 1, pp. 1–12, 2019.

[25] D. Woods, I. Agrafiotis, J. R. C. Nurse, and S. Creese, "Mapping the coverage of security controls in cyber insurance proposal forms," *Journal of Internet Services and Applications*, vol. 8, no. 1, Dec. 2017, doi: 10.1186/s13174-017-0059-y.

[26] S. Groš, "A Critical View on CIS Controls," in *2021 16th International Conference on Telecommunications (ConTEL)*, Oct. 2021, pp. 122–128. doi: 10.23919/ConTEL52528.2021.9495982.

[27] Center for Internet Security (Inc), "CIS Controls Cloud Companion Guide v8 CIS Controls Cloud Companion Guide," 2022. [Online]. Available: http://www.cisecurity.

[28] T. Casey, K. Fiftal, K. Landfield, J. Miller, D. Morgan, and B. Willis, "The Cybersecurity Framework in Action: An Intel Use Case," 2015.

[29] W. Alkalabi, L. Simpson, and H. Morarji, "Barriers and Incentives to Cybersecurity Threat Information Sharing in Developing Countries: A Case Study of Saudi Arabia," in *2021 Australasian Computer Science Week Multiconference*, New York, NY, USA: ACM, Feb. 2021, pp. 1–8. doi: 10.1145/3437378.3437391.