MANAJEMEN INDIKATOR KEAMANAN INFORMASI DI BAWAH MODEL KEAMANAN KOGNITIF

Barzan Trio Putra

Jurusan Sistem Komputer, Universitas Sriwijaya
JL. Masjid Al Ghazali, Bukit Lama, Kec Ilir Barat I, Kota Palembang, Sumatera Selatan 30128, Indonesia

E-mail : barzan.tp14@gmail.com

Abstract

Organizations face daily different computer security threats, which makes necessary to have a Decision Support System (DSS) that allows generating knowledge to define strategies to minimize risk. The information security management supported in DSS requires time-consuming manual processes, analysis of large amounts of data and the experience of security specialists. The use of alternatives such as bigdata, machine learning, data analytics, and data visualization can reduce the time of manual processes and the automation of data analysis, contributing the inclusion of intelligence to decision support systems. This study presents a conceptual framework based on the three components of information security: people, technology and processes, with a cognitive approach; emphasizing the aspect of technology in the management of indicators through the integration of concepts such as bigdata, machine learning, data analytics, and data visualization to strengthen the DSS for the generation of knowledge and to help security specialists to make decisions at a strategic level.

Keywords : security management system, Decision Support System, Data visualization, information Security

Abstrak

Organisasi menghadapi keamanan komputer yang berbeda setiap hari ancaman, yang diperlukan untuk memiliki Sistem Pendukung Keputusan (DSS) yang memungkinkan menghasilkan pengetahuan untuk menentukan strategi meminimalkan risiko. Manajemen keamanan informasi didukung dalam DSS membutuhkan proses manual yang memakan waktu, analisis sejumlah besar data dan pengalaman spesialis keamanan. Penggunaan alternatif seperti bigdata, pembelajaran mesin, data analitik, dan visualisasi data dapat mengurangi waktu manual proses dan otomatisasi analisis data, berkontribusi dimasukkannya intelijen ke sistem pendukung keputusan. Pelajaran ini menyajikan kerangka kerja konseptual berdasarkan tiga komponen keamanan informasi: orang, teknologi dan proses, dengan pendekatan kognitif; menekankan aspek teknologi dalam pengelolaan indikator melalui integrasi konsep seperti bigdata, pembelajaran mesin, analitik data, dan visualisasi data untuk memperkuat DSS untuk generasi pengetahuan dan untuk membantu spesialis keamanan untuk membuat keputusan tingkat strategis.

Kata Kunci : security management system, sistem pendukung keputusan

1. Pendahuluan

Keamanan informasi didefinisikan oleh National Institute of Standar dan Teknologi - NIST, seperti perlindungan sistem informasi dan komputer, akses tidak sah, penggunaan, gangguan,

pengungkapan atau modifikasi untuk menjamin kerahasiaan, ketersediaan, dan integritas . Selama 2016, SYMANTEC telah mendeteksi sekitar 1200 pelanggaran keamanan, 1.1 miliar identitas terpapar, 463.841 deteksi ransomware, dan sekitar 229.000 serangan web per hari . Di bawah konteks ini, organisasi harus membentuk metodologi, didokumentasikan dan proses terukur yang memungkinkan analisis, implementasi, pemantauan dan peningkatan kontrol, tindakan dan prosedur di tingkat operasional, taktis dan strategis keamanan, untuk menjamin keandalan, integritas dan ketersediaan informasi. Proses metodologis ini dikenal sebagai manajemen keamanan informasi memerlukan definisi indikator yang memungkinkan mengevaluasi efektivitas dan efisiensi berbagai komponen yang terlibat dalam keamanan di bawah norma dan standar[3].

Keamanan informasi proses manajemen umumnya melibatkan proses manual mengumpulkan informasi dan analisis kepatuhan secara terperinci dengan daftar metrik keamanan, yang melibatkan indikator seperti: kembalinya solusi keamanan, analisis malware, kerentanan analisis, analisis forensik, antara lain. tujuan yaitu mengintegrasikan penggunaan kecerdasan buatan, bigdata, analitik data dan visualisasi data di bidang cybersecurity, di bawah konsep keamanan kognitif [5]. Dalam arti ini, penting untuk mempertimbangkan Sistem Pendukung Keputusan (DSS) dalam organisasi untuk pengelolaan indikator, itu harus diintegrasikan dan dirancang dengan pendekatan kognitif di mana kemampuan beradaptasi, skalabilitas, dan konsumsi sumber daya komputasi yang rendah diperlukan. Selain itu, integrasi solusi keamanan kognitif harus bertemu pada titik di mana organisasi memusatkan peristiwa keamanan, jadi alternatifnya seperti Pusat Operasi Keamanan (SOC) atau Komputer Tim Respons Insiden Keamanan (CSIRT) juga dipertimbangkan. Untuk alasan ini, kontribusi utama dari pekerjaan ini adalah untuk menghasilkan kerangka kerja yang memungkinkan pembentukan informasi indikator keamanan difokuskan pada metodologi analisis risiko, yang memungkinkan untuk mengkategorikan analisis keamanan, tentukan keterampilan spesialis keamanan dan menyajikan informasi yang lebih besar relevansi dengan pembuat keputusan.

Penelitian ini mempertimbangkan pendekatan kognitif, di mana istilah Keputusan Cerdas Sistem Pendukung (IDSS) [6] akan diadopsi, yang membahas DSS yang dikembangkan berdasarkan pengambilan keputusan kognitif didukung oleh penggunaan kecerdasan buatan. Penelitian ini mengusulkan kerangka kerja konseptual di bawah pendekatan kognitif yang mengintegrasikan solusi keamanan kognitif di Pusat Operasi Keamanan dengan tujuan memiliki pemantauan real-time indikator manajemen keamanan informasi, dan implementasi Pusat Operasi Keamanan Kognitif yang akan menjadi pusat dari keputusan cerdas sistem pendukung - IDSS di tingkat strategis organisasi.

2. Metode

Tujuan dari makalah ini adalah untuk menyajikan kerangka kerja konseptual di bawah pendekatan keamanan kognitif untuk mengotomatisasi validasi metrik dari perspektif manajemen indikator keamanan informasi secara real time. Itu juga diusulkan untuk menganalisis Pusat Operasi Keamanan (SOC), dan peran analis keamanan, dari perspektif kognitif. Dalam hal ini, Kowtha et al[7]. menunjukkan pentingnya menentukan metodologi untuk pengumpulan dan visualisasi informasi dari berbagai sumber informasi. Sebuah pekerjaan terkait ditemukan di sekitar analisis keragaman lingkungan dunia maya dan karenanya berbeda masalah dan solusinya[5]. Penulis mengusulkan model kerja untuk manajemen insiden yang memungkinkan pengumpulan dan visualisasi informasi yang menghasilkan pengetahuan untuk pengambilan keputusan, didukung oleh keputusan sistem pendukung untuk keamanan siber. Menurut Holapple dan Clyde DSS dapat diklasifikasikan ke dalam enam kerangka kerja: berorientasi teks, berorientasi database, berorientasi spreadsheet, solverorien, berorientasi aturan, dan gabungan. Dalam praktiknya, untuk memiliki DSS hibrida yang mengandung setidaknya dua kerangka kerja yang disebutkan memberikan pengetahuan yang lebih baik untuk pengambilan keputusan. Dari perspektif mendefinisikan kerangka kerja yang mendukung IDSS kami untuk keamanan siber, kami menganalisis beberapa solusi itu menghasilkan pengetahuan berdasarkan analisis peristiwa keamanan dengan penggunaan solusi kognitif.

dapat disimpulkan bahwa dalam manajemen keamanan informasi, analis keamanan memerlukan keterampilan khusus baru sebagaimana dianalisis dalam Informasi SANS Pelatihan Keamanan, dalam publikasi “Visualisasi Data Keamanan” [6], menghasilkan peran baru dalam

keamanan siber yang disebut Cyber Ilmuwan Data Keamanan. Seperti disebutkan sebelumnya, ada beberapa proposal yang ditampilkan penggunaan solusi kognitif dalam lingkup cybersecurity, tetapi itu didistribusikan di berbagai bidang seperti keamanan visualisasi, kecerdasan buatan dalam cybersecurity atau bigdata dalam cybersecurity. Solusi ini bertujuan untuk menghasilkan alternative pada tingkat keamanan informasi operasional dan taktis. Seperti yang dinyatakan sebelumnya, ada beberapa proposal yang menganalisis penggunaan pembelajaran mesin, data besar, analisis data, dan data visualisasi untuk mengotomatisasi dan memvisualisasikan analisis keamanan peristiwa dan pola lalu lintas di jaringan, yang saat bekerja di bawah proposal independen mungkin tidak menghasilkan pengetahuan di tingkat strategis untuk pengambilan keputusan. Dalam pengertian ini, ada kebutuhan untuk mengintegrasikan solusi yang diusulkan ini dan fokus pada generasi pengetahuan untuk tingkat informasi strategis keamanan. IDSS yang dibutuhkan dalam konteks ini disesuaikan dengan kerangka kerja untuk mana model konseptual diusulkan, di mana proposal yang berbeda dianalisis, menjaga kognitif pendekatan dan memungkinkan generasi pengetahuan di tingkat strategis.

3. Landasan Teori

Manajemen informasi keamanan memerlukan tiga komponen utama untuk operasinya: proses, orang dan teknologi. Jika kita mempertimbangkan penggunaan keamanan kognitif untuk komponen ini, dapat disimpulkan bahwa tiga komponen juga harus menyelaraskan diri dengan pendekatan kognitif baru ini, karena ditunjukkan pada Gambar 1. Mengenai proses komponen, ini membahas manajemen keamanan informasi di bawah standar yang ada seperti ISO 27000 series, ISO 38500, panduan referensi NIST atau kerangka kerja tata kelola COBIT. Karena itu, pekerjaan ini tidak akan menganalisis secara terperinci manajemen keamanan informasi model, sebagai gantinya akan difokuskan pada implementasi indikator keamanan manajemen dan metrik keamanan, mempertimbangkan teknologi yang muncul seperti IoT dan Cloud. Dari pendekatan kognitif, proses yang didefinisikan oleh organisasi harus memasukkan privasi pengguna dalam penambangan data, bigdata, pembelajaran mesin atau visualisasi data.

Proposal yang disajikan mempertimbangkan kerangka kerja konseptual yang dapat diterapkan untuk organisasi yang berbeda, di mana lapisan yang berbeda didefinisikan untuk mengevaluasi komponen kognitif terkait dengan pembelajaran mesin, bigdata, analisis data, dan data visualisasi, seperti yang ditunjukkan pada Gambar 2. Beberapa alternatif teknis diusulkan yang dapat dipertimbangkan dalam setiap lapisan mereka tidak eksklusif atau terkondisi.

A. Komponen Teknologi Di Bawah Pendekatan Kognitif

Mempertimbangkan bahwa solusi berbeda yang ditemukan dalam literatur milik bidang teknologi yang berbeda seperti mesin pembelajaran, bigdata, analitik data dan visualisasi data, kerangka kerja konseptual berdasarkan lapisan diusulkan yang memungkinkan penerapan Sistem Pendukung Keputusan Cerdas untuk manajemen indikator mempertimbangkan kerangka gabungan [5] Lapisan Pusat Operasi Keamanan Kognitif dijelaskan di bawah ini:

1) **Information source Layer :** Lapisan ini mempertimbangkan berbagai peralatan yang membentuk jaringan seperti: server, peralatan jaringan, peralatan keamanan perimeter, peralatan pengguna dan peralatan IoT, yang menghasilkan aliran data antara mesin ke mesin (M2M), mesin ke pengguna (M2U) atau sistem ke sistem (S2S), produk dari interaksi yang berbeda. Untuk proses implementasi lapisan ini dianggap identifikasi semua perangkat, sistem atau pengguna yang merupakan bagian dari jaringan, sehingga perlu mempertimbangkan tingkat detail nama pengguna, nama mesin, alamat IP, alamat MAC, di antara Informasi lainnya. Ini juga dianggap sebagai implementasi dari berbagai solusi untuk pembuatan rekaman, seperti aktivasi catatan di server atau pemasangan monitor agen atau detektor intrusi di tingkat tuan rumah. Lapisan ini adalah satu dari yang paling relevan karena jika beberapa informasi dibuang, blind-spot informasi akan dibuat dimana serangan itu tidak diketahui oleh analis keamanan dapat dihasilkan.

2) **Sensor Layer** : Lapisan ini menetapkan penggunaan keamanan sensor yang memungkinkan untuk menghasilkan peringatan saat mendeteksi anomaly tingkah laku. Implementasi lapisan ini penting

karena ada perangkat yang tidak memiliki agen, jadi mungkin ada hilangnya informasi untuk analisis, sebaliknya, itu dianggap untuk mengimbangi dengan sensor yang diterapkan secara terdistribusi (pemantauan terdistribusi). Juga, perlu untuk memantau aliran data dalam jaringan dan menetapkan level tertentu pola pembelajaran yang tidak mudah dirasakan oleh analis keamanan. Untuk membangun kecerdasan dalam sensor dan jaringan kognitif, algoritma pembelajaran mesin diterapkan untuk menganalisis perilaku atau pola anomali sebagai serta informasi pertukaran data antar sensor. Di lapisan ini menggunakan algoritma pembelajaran tanpa pengawasan, seperti K-means, atau jaringan kognitif lebih dapat diterapkan, karena perlu untuk mempertimbangkan seluruh rangkaian sensor sebagai bagian dari jaringan pemantauan dan tidak diperlakukan secara independen. Penerapan pembelajaran terbimbing sebagai pohon keputusan diuji dalam proposal tetapi tidak memberikan kontribusi yang relevan karena itu tergantung pada pengalaman analis keamanan dan pada lapisan ini minatnya adalah mendeteksi kemungkinan anomaly perilaku tidak terdeteksi. Alat seperti WEKA, MATLAB atau dapat digunakan di lapisan ini. Mempertimbangkan konsumsi sumber daya pemrosesan, proposal kami menggunakan komputer mini, seperti raspberry, untuk implementasi sensor, jadi pemrosesan akan didistribusikan dan harus dianggap sebagai master node dari sensor jika

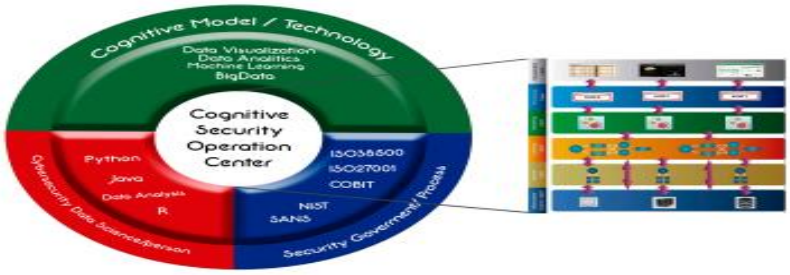

Figure 1. Proposed Model: Components for Information Security Management

membutuhkan pemrosesan yang lebih besar untuk jaringan kognitif.

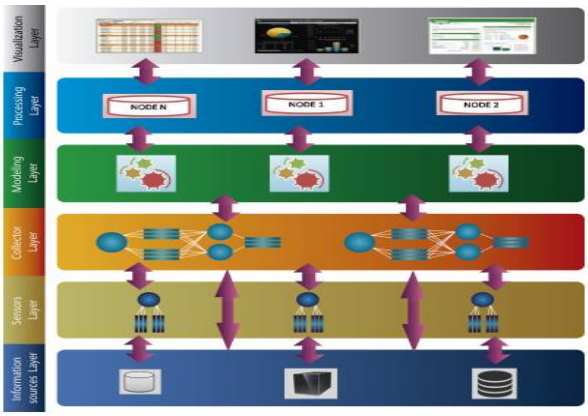

Figure 2. Layers in the Cognitive Security Operation Center

3) **Collection Layer** : Pada tahap ini, koleksi informasi yang dihasilkan oleh sensor dan sumber informasi dilakukan. Mengingat bahwa ada sejumlah besar data yang terlibat dan diperlukan analisis waktu nyata, penggunaan solusi bigdata diusulkan untuk proses ini seperti Logstatsh atau ElasticSearch.

4) **Modeling Layer** : Pada layer ini perlu untuk dibawa keluar pemodelan informasi yang dikumpulkan, untuk menggambarkan aliran data dan untuk menetapkan jenis paling umum interaksi yang ada di dalam jaringan. Ini akan memungkinkan untuk mendefinisikan kembali lokasi sensor baru dan mengidentifikasi kemungkinan pelanggaran keamanan. Tahap ini membutuhkan interelasi dari

pengalaman analis keamanan, administrator jaringan dan administrator server untuk membangun aliran data yang dimiliki parameter perilaku normal. Di lapisan ini, diusulkan untuk melakukan pra-laporan menggunakan solusi seperti Kibana, untuk menganalisis informasi yang diperoleh dari lapisan koleksi.

5) **Processing Layer** : Lapisan ini juga menggunakan pembelajaran mesin solusi dengan tujuan menganalisis perilaku anomaly atau parameter dalam jaringan. Lapisan ini menyediakan master simpul untuk jaringan kognitif sensor. Itu dibagi menjadi dua tingkat pemrosesan. Tahap pertama diusulkan menggunakan algoritma tanpa pengawasan yang menggunakan informasi yang dihasilkan di lapisan sebelumnya. Tujuannya adalah untuk melakukan analisis dari informasi yang dihasilkan oleh jaringan kognitif sensor dan untuk mendapatkan informasi yang tidak diketahui oleh pihak keamanan analis mengenai pola perilaku anomali. Tahap kedua terdiri dari algoritma yang diawasi di mana beberapa kritis tujuan jaringan didefinisikan sebagai server, jaringan peralatan distribusi dan generasi berbasis pengetahuan pada tujuan yang ditetapkan. Lapisan ini bertanggung jawab untuk mengoordinasi kecerdasan sensor terdistribusi sesuaikan dengan kondisi baru atau pola yang terdeteksi.

6) **Visualization Layer**: Pada lapisan ini visualisasi informasi yang dihasilkan oleh lapisan pemrosesan disajikan. Lapisan ini memungkinkan analis keamanan untuk mengamati aliran data, serangan paling umum yang telah diterima, terdeteksi pola dan kemungkinan pelanggaran keamanan. Penting dalam hal ini layer untuk membuat model grafik interaktif yang memungkinkan untuk merepresentasikan informasi yang dihasilkan dengan cara yang jelas dan efektif lapisan yang berbeda. Lapisan ini adalah yang relevan kedua, sejak itu berinteraksi langsung dengan analis keamanan. Itu perlu pertimbangkan di lapisan ini atribut kapan, apa dan di mana, sehubungan dengan aliran data jaringan, analisis port digunakan dalam komunikasi jaringan, memvisualisasikan paket dan hubungan di antara mereka; dan untuk menyajikan visualisasi geolokasi mempertimbangkan perluasan jaringan. Akhirnya, tentang visualisasi, warna dan waktu respons persepsi visual manusia akan dipertimbangkan.

4. Pembahasan

Organisasi publik dan swasta dipaksa untuk memberikan jaminan keandalan, integritas, dan ketersediaan informasi dalam kepatuhan terhadap hukum setempat, nasional dan internasional dan peraturan seperti: Hak dan Privasi Pendidikan Keluarga Act (FERPA), Keamanan Data Industri Kartu Pembayaran Standar (PCI-DSS) [5], Portabilitas Asuransi Kesehatan dan Akuntabilitas Act (HIPAA) [30], atau UU Peluang Pendidikan Tinggi (HEOA) [1], yang membutuhkan informasi manajemen keamanan yang memungkinkan untuk membuat strategi proaktif terhadap ancaman atau serangan keamanan yang dapat memengaruhi organisasi. Untuk menetapkan alternatif yang memungkinkan migrasi dari metodologi mitigasi risiko, di mana penggunaan strategi korektif atau preventif maksimum untuk insiden keamanan adalah lebih disukai, untuk metodologi minimisasi risiko, di mana proaktif Diperlukan strategi keamanan, karena mengurangi dampaknya pada organisasi, serta biaya yang terlibat dalam penyelesaian insiden keamanan, melibatkan generasi pengetahuan di Indonesia waktu nyata di tingkat strategis. Ini mengarah ke dalam DSS tingkat kecerdasan, kemampuan beradaptasi dan skalabilitas. Karya-karya [3], memberikan pentingnya mengelola solusi visualisasi yang sederhana, interaktif dan mudah dipahami oleh analis keamanan yang harus berurusan dengan sejumlah besar peringatan dari tim keamanan, analisis sejumlah besar data dalam arus lalu lintas untuk mendeteksi anomali dan menekankan perlunya mengotomatisasi proses analisis ini. Pendekatan yang berpusat pada pengguna ini sangat ideal mengingat fisik keterbatasan manusia, seperti kelelahan setelah beberapa jam pemantauan, subjektivitas yang bisa dibuat setelah membaca beberapa log, dan pengalaman diperlukan. Di sisi lain, studi pertimbangkan secara rinci penerapan visualisasi data, pembelajaran mesin dan solusi penambangan data untuk analisis peristiwa keamanan atau pola anomali dalam lalu lintas jaringan, yang melengkapi proposal visualisasi dianalisis. Kontribusi ini berusaha untuk memecahkan masalah analis keamanan yang bekerja dengan besar jumlah data. Penggunaan pembelajaran mesin, data besar, data analitik dan visualisasi data, secara kolektif disebut sebagai keamanan kognitif, adalah alternatif yang sangat layak untuk menghasilkan

pengetahuan pengambilan keputusan dan penerapan Sistem Pendukung Keputusan Cerdas. Namun demikian, ketika mempertimbangkan pendekatan kognitif diperlukan untuk menekankan terutama dalam manusia, dalam persepsinya, pemikirannya, caranya bertindak, seperti yang dianalisis oleh karya "Perspektif tentang peran kognisi dalam cybersecurity, di mana penekanan diberikan pada kebutuhan menggabungkan media teknologi dengan perspektif dan memikirkan manusia.

Dari pekerjaan terkait, beberapa kontribusi bisa jadi diekstraksi dalam penerapan keamanan kognitif, tetapi itu diperlukan untuk menyatukan berbagai proposal di bawah pendekatan kognitif tunggal, yang mendukung tingkat strategis di mana keputusan dibuat. Mengkonsolidasikan proposal ini di generasi Sistem Pendukung Keputusan Cerdas, di sana adalah kebutuhan yang akan menjadi prioritas tinggi di masa depan untuk organisasi, mengingat sejumlah besar peralatan yang terhubung, generasi layanan baru di Internet dan peran pengguna setiap kali semakin aktif di dunia maya. Proposal yang disajikan mengintegrasikan berbagai proposal yang memanfaatkan keamanan kognitif di bawah kerangka kerja konseptual, tetapi di luar itu, itu bertujuan untuk menyoroti keselarasan dibutuhkan oleh para aktor manajemen keamanan informasi, orang, teknologi, dan proses di bawah pendekatan kognitif ini. Alternatif seperti Ilmu Data Keamanan Cyber harus dianalisis oleh organisasi dalam kognitif saat ini era yang sedang muncul. Dari perspektif ini kontribusi pekerjaan ini untuk mengubah fokus Operasi Keamanan Pusat pendekatan kognitif yang menghasilkan pengetahuan di waktu nyata untuk pengambilan keputusan strategis.

5. Kesimpulan

Proposal dalam penelitian ini, menjawab pertanyaan penelitian, cara mengurangi waktu untuk mengevaluasi keamanan informasi indikator manajemen? melalui definisi konseptual kerangka kerja untuk otomatisasi validasi metrik dari perspektif manajemen keamanan informasi indikator secara real time. Kerangka yang diusulkan mempertimbangkan DSS, analisis Pusat Operasi Keamanan, dan perannya analis keamanan, dari pendekatan kognitif. Berbasis pada struktur lapisan yang menggambarkan komponen yang berbeda yang memungkinkan menghasilkan pengetahuan di tingkat strategis secara nyata waktu di bawah konsep DSS Cerdas. DSS melakukan pengambilan keputusan di tingkat strategis organisasi. Mereka dibangun berdasarkan data historis, pemantauan peristiwa waktu nyata, dan basis pengetahuan yang dihasilkan oleh pengalaman spesialis keamanan. Mengingat besar jumlah data yang dihasilkan untuk acara keamanan, dan dinamika di dunia maya, diperlukan bahwa DSS dapat diadaptasi segera untuk variasi variabel yang berbeda dari organisasi tempat metrik dan indikator informasi keamanan dibuat. Pusat Operasi Keamanan, yang mendukung Intelligent DSS, di bawah pendekatan kognitif, juga mempertimbangkan pentingnya manusia, pengalamannya, kemampuan dan pengetahuan substantif. Implementasinya othat fokus pada penggunaan keamanan kognitif harus difokuskan tentang penyediaan aksesibilitas kepada pengguna, dalam hal ini, keamanan analis dan pembuat keputusan. Mempertimbangkan itu alternatif-alternatif teknologi ini tidak menggantikan manusia menjadi tetapi menjadi pelengkap dengan tugas operatif dan memungkinkan spesialis keamanan untuk fokus pada analisis strategis ketika memiliki visi organisasi yang komprehensif. Itu Penerapan model kognitif melibatkan otomatisasi proses pengumpulan data, pemrosesan dan transformasi menggunakan pembelajaran mesin, analisis data, atau visualisasi data, dan juga mempertimbangkan integrasi dari alternatif ini ke generasi pengetahuan untuk pengambilan keputusan dan focus pada kognisi manusia, mempertimbangkan analisis pengguna perilaku dalam penggunaan sistem komputer, dan pengalaman analis keamanan.

6. Referensi

[1] R. Andrade, J. Torres, and P. Flores, “Management of information security indicators under a cognitive security model,” in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, 2018, pp. 478–483.

[2] R. O. Andrade and S. G. Yoo, “Cognitive security: A comprehensive study of cognitive science in cybersecurity,” *J. Inf. Secur. Appl.*, vol. 48, p. 102352, 2019.

[3] R. R. Gutta, “Managing Security Objectives for Effective Organizational Performance Information Security Management,” Walden University, 2019.

[4] R. Andrade and J. Torres, “Self-Awareness as an enabler of Cognitive Security,” in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2018, pp. 701–708.

[5] R. O. Andrade *et al.*, “Information Security Management in University Campus Using Cognitive Security,” *Int. J. Comput. Sci. Secur.*, vol. 13, no. 4, p. 124, 2019.

[6] R. Andrade, J. Torres, and L. Tello-Oquendo, “Cognitive Security Tasks Using Big Data Tools,” in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2018, pp. 100–105.

[7] E. W. B. Anderson, A. Murray, and A. Spiers, “System and method for providing scorecards to visualize services in an intelligent workload management system.” Google Patents, 2015.