Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202183123
Vol. 8, No. 6, Desember 2021, hlm. 1137-1148 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA JARINGAN (STUDI KASUS : UIN SUNAN KALIJAGA YOGYAKARTA)

Rizki Dewantara*[1], Bambang Sugiantoro[2]

[1,2] Universitas Islam Negeri Sunan Kalijaga, Yogyakarta
Email: [1]dewantararizki@gmail.com, [2]bambang.sugiantoro@uin-suka.ac.id
*Penulis Korespondensi

(Naskah masuk: 20 Januari 2020, diterima untuk diterbitkan: 15 November 2021)

Abstrak

Serangan pada jaringan saat ini sangat sering terjadi, dengan semakin banyaknya cara untuk melakukan pengaksesan terhadap data dan semakin berkembangnya teknologi yang digunakan tentunya akan menyebabkan meningkatnya ancaman keamanan suatu jaringan. Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (KAMI) yang dilakukan pada jaringan di UIN Sunan Kalijaga Yogyakarta didapatkan hasil indeks 407, yang dianggap masih belum optimal. Hal ini yang mendasari perlunya implementasi Open Source SIEM (OSSIM) ke dalam indeks KAMI. Penelitian ini dilakukan untuk mengoptimalkan proses keamanan informasi agar dapat bekerja sesuai dengan standar indeks KAMI. Metode penelitian yang digunakan meliputi studi literatur, melakukan Pre-Assesment Indeks KAMI, mengimplementasi infrastruktur OSSIM, monitoring indeks keamanan informasi menggunakan teknologi OSSIM, dan melakukan Post-Assesment Indeks KAMI, tahapan akhir ini menganalisis hasil monitoring untuk dibuat perbandingan bagaimana kondisi jaringan sebelum dan sesudah diimplementasikan OSSIM pada jaringan. Skor nilai perbandingan dari hasil penelitian terkait Indeks KAMI menunjukkan peningkatan skor penilaian sebesar 25, setelah diterapkan penggunaan OSSIM dari sebelumnya tanpa penerapan OSSIM sebesar nilai 407 menjadi 432. Peningkatan indeks KAMI membantu menaikan nilai pada aspek tata kelola, pengelolaan asset dan teknologi, namun tingkat kelayakan keamanan informasi masih di level I+ sampai dengan II+ sehingga keamanan informasi pada jaringan tidak layak dan butuh perbaikan.

Kata kunci: Indeks *KAMI*, Keamanan Informasi, *Open Source SIEM* (OSSIM)

EVALUATION OF INFORMATION SECURITY MANAGEMENT USING INFORMATION SECURITY INDEX (KAMI) ON THE NETWORKS (CASE STUDY: UIN SUNAN KALIJAGA YOGYAKARTA)

Abstract

Attacks on networks today are very common, with more and more ways to access data and the development of technology used, they will certainly cause an increase in network security threats. Evaluation of information security management using the information security index (KAMI) conducted on the network at UIN Sunan Kalijaga Yogyakarta obtained an index result of 407, which is considered still not optimal. This underlies the need to implement Open Source SIEM (OSSIM) into the KAMI index. This research was conducted to optimize the information security process so that it can work according to the KAMI index standards. The research methods used include literature study, conducting KAMI Index Pre-Assessment, implementing OSSIM infrastructure, monitoring information security index using OSSIM technology and conducting KAMI Index Post-Assessment, this final stage analyzes the results of monitoring to make comparisons of network conditions before and after implementation of OSSIM on the network. Comparative scores from the results of research related to the KAMI Index show an increase in the score of 25, after applying OSSIM from before without applying OSSIM, the value of 407 becomes 432. The increase in the KAMI index helps raise the value of governance aspects, asset management and technology, but the level of information security eligibility is still at the level of I+ to II+ so the information security on the network is not feasible and needs improvement.

Keywords: *KAMI Index, Information Security, Open Source SIEM (OSSIM)*

1. PENDAHULUAN

Sistem deteksi penyusupan telah berkembang seiring dengan berkembangnya tantangan dan permasalahan yang perlu diakomodasi oleh sistem tersebut (Sugiantoro, 2017). Kebutuhan instansi pemerintahan untuk menerapkan Standar Managemen Keamanan Informasi sesuai dengan Sistem Manajemen Keamanan Informasi (SMKI) dan monitoring terhadap jaringan menjadi pilihan yang mutlak agar *security officer* dapat dengan jelas melihat apa yang terjadi dengan jaringannya. (MENKOMINFO, 2019).

Open Source Security Information Management (OSSIM) adalah sebuah *Platform Security Information Management* yang berbasiskan *open source* dan merupakan kumpulan lebih dari 15 *open source security program* yang semuanya terkandung di dalam sistem ini untuk menghasilkan kontrol manajemen keamanan pada sebuah jaringan (Hadiansyah chandra and Iskandar, 2017). Sedangkan Indeks Keamanan Informasi (KAMI) merupakan suatu alat untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan SNI *ISO/IEC* 27001:200 serta peta *area* tata kelola keamanan sistem informasi di suatu lembaga pemerintahan. Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan IT dalam mendukung terlaksananya tugas pokok dan fungsi yang ada. Indeks penilaian keamanan informasi untuk mengukur kematangan manajeman keamanan layanan TI yaitu semakin tinggi ketergantungan terhadap TIK maka harus semakin banyak bentuk pengamanan yang di terapkan sampai tahap tertinggi (Lenawati, Winarno and Amborowati, 2017). Berdasarkan pada penilaian resiko bahwa resiko bernilai ekstrim adalah kehilangan integritas informasi, kegagalan perangkat dan layanan, gangguan komunikasi, dan kegagalan sistem/alat sehingga dibuatkan kontrol akses yang berkaitan dengan *asset* tersebut. Untuk menangani masalah ini, MENKOMINFO memperkenalkan Indeks KAMI sebagai alat untuk menilai tingkat kematangan institusi untuk memenuhi informasi nasional standar manajemen keamanan. Sebelum standar keamanan informasi diterapkan, perlu dilakukan evaluasi *system* keamanan informasi di jaringan UIN Sunan Kalijaga Yogyakarta untuk mendapatkan gambaran kondisi kesiapan dan kematangan manajemen keamanan informasi tersebut. Dalam pelaksanaan pengukuran tingkat kematangan manajemen keamanan informasi pada jaringan UIN Sunan Kalijaga Yogyakarta mengunakan model yang di siapkan oleh Kominfo RI tahun 2019, yaitu indeks KAMI. Indeks KAMI dibuat dengan acuan *ISO* 27001:2018 yang berisi tentang keamanan informasi. *ISO* 27001 adalah suatu bentuk kerangka kerja standar internasional yang berisi tentang standar-standar dalam *area* keamanan informasi, lingkup penggunaan teknologi dan pengelolaan *asset* yang membantu organisasi memastikan bahwa keamanan informasi sudah berjalan dengan efektif (ISO/IEC, 2018). Dibutuhkan upaya-upaya besar untuk memperbaiki keamanan informasi di lembaga pemerintahan untuk menerapkan kontrol dasar risiko dan juga dari strategi keamanan informasi. *Data* yang digunakan dalam evaluasi ini nantinya akan memberikan gambaran indeks kesiapan keamanan informasi dari aspek kelengkapan maupun kematangan, kerangka kerja, keamanan informasi yang diterapkan yang dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

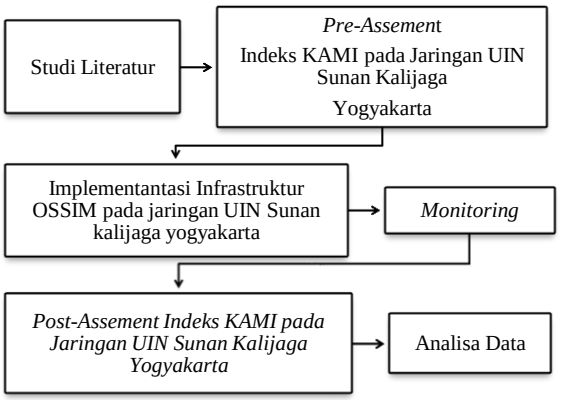
Beberapa penelitian pernah dilakukan terkait evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi diantaranya Angga Juansyah, Bagus Pratama (2018) pernah melakukan penelitian tentang implementasi OSSIM pada keamanan jaringan komputer di PT. Satria Antaran Prima Palembang dan mendeteksi aktifitas *pingflood* dan aktifitas pengaksesan *router* yang dilakukan oleh *host* dalam jaringan Perusahaan ini. OSSIM yang diimplementasi hanya mampu mendeteksi serangan atau sebagai IDS. (Angga Juansyah, Bagus Pratama, 2018). Selanjutnya penelitian yang dilakukan oleh Putra dan Tjahjadi (2018) membahas tentang Indeks KAMI yang dilakukan dengan melakukan evaluasi keamanan informasi pada perguruan tinggi, untuk mendapatkan sertifikasi *ISO/IEC* 27001:2009 *level* keamanan informasi adalah minimal III (Putra and Tjahjadi, 2018). Penelitian selanjutnya dilakukan oleh (Pratama, dkk (2018) yang membahas evaluasi tata kelola sistem keamanan teknologi informasi menggunakan indeks KAMI dan *ISO* 27001 bahwa tingkat kematangan dan keamanan informasi KOMINFO masih tergolong rendah karena KOMINFO masih dalam perencanaan atau belum mengaplikasikan syarat - syarat keamanan informasi (Pratama, Suprapto and Perdanakusuma, 2018). Kemudian penelitian tentang Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya yang dilakukan oleh (Basyarahil, dkk (2017), pada penelitian tersebut mengungkapkan hasil diantaranya belum dapat dikatakan matang dan sesuai dengan standar ISO 27001:2013 karena belum mencapai *level* III+ dimana penerapan keamanan informasi telah terdefinisi dan konsisten (Basyarahil, Astuti and Hidayanto, 2017). Kemudian penelitian tentang Pengukuran Keamanan Informasi PDAM Titra Medal Menggunakan Indeks KAMI Untuk Analisis Tingkat Kematangan Keamanan Informasi yang dilakukan oleh (Sutara, (2018), pada penelitian ini pihak instansi telah menyadari betul bahwa peran teknologi atau TIK sudah sangat jelas memberikan

kemudahan bagi para *staff* untuk membantu menjalankan proses bisnis. Perubahan pada keamanan informasi pada intansi dilakukan dengan wawancara dengan kuesioner pada analis jaringan pada suatu intansi agar diketahui celah keamanan informasi (Sutara, 2018). Kemudian penelitian oleh (Akhirina, dkk (2016) mengenai Evaluasi Keamanan Teknologi Informasi Pada PT Indotama *Partner Logistics* menggunakan Indeks KAMI yang berada di level I+ sampai dengan II+, Hasil dari evaluasi di PT Indotama *Partners Logistics* terhadap TIK masih belum dilaksanakan secara menyeluruh dan konsisten, akan tetapi masih ditahap penerapan sebagian dan dalam perencanaan (Akhirina, Arif and and Rahmatika, 2016). Kemudian penelitian tentang Indeks Penilaian Keamanan Informasi Untuk Mengukur Kematangan Manajeman Keamanan Layanan TI (Studi Kasus :BPMP Kabupaten Gresik) yang dilakukan oleh (Hidayat, dkk (2018), dengan hasil yaitu semakin tinggi ketergantungan terhadap TIK atau semakin penting peran TIK maka harus semakin banyak bentuk pengamanan yang di perlukan dan harus di terapkan sampai tahap tertinggi (Hidayat, Suyanto and Sunyoto, 2018).

Berdasarkan penelitian-penelitian sebelumnya, peneliti melakukan penggalian terkait konsep dan mengimplementasikan penggunaan OSSIM untuk evaluasi manajemen terhadap peningkatan keamanan informasi di UIN Sunan Kalijaga Yogyakarta dengan menciptakan sistem pendeteksi atau *sensor* terhadap *area* jaringan menggunakan aplikasi berbasis *open source*, yaitu *alientvault* OSSIM sehingga memberikan laporan kepada administrator sistem mengenai upaya penyerangan terhadap sistem, melalui catatan atau log yang dihasilkan oleh aplikasi sebagai bukti digital yang mencatat segala upaya penyerangan atau penetrasi ke dalam suatu *area* server. Tujuan dari penelitian ini yaitu memantau dan mengetahui lebih detail permasalahan yang ada pada jaringan UIN Sunan Kalijaga Yogyakarta sehingga dapat diketahui pola solusi untuk mengatasinya kemudian memaksimalkan infrastruktur jaringan komputer yang ada dengan lebih efektif dan efisien sesuai fungsinya sebagai institusi pendidikan, hasilnya dapat digunakan sebagai bahan pertimbangan dalam rangka menyusun langkah-langkah perbaikan manajemen keamanan sistem informasi pada Sistem Informasi UIN Sunan Kalijaga Yogyakarta. Tingkat kelayakan yang rata-rata menduduki level I+ dan II+ tanpa penerapan OSSIM sebesar nilai 407 melalui kuesioner *pre-assesment* indeks KAMI kepada responden menunjukkan kesiapan sertifikasi masih dikatakan belum layak sertifikasi keamanan informasi, karena untuk mencapai batas minimum kesiapan sertifikasi keamanan informasi adalah tingkat III sehingga diterapkan *Open Source* SIEM (OSSIM) untuk diimplementasikan didalam Infrastruktur Jaringan UIN Sunan Kalijaga Yogyakarta sehingga dapat meningkatkan indeks KAMI.

2. METODE PENELITIAN

Tahapan yang akan dilakukan dalam penelitian terkait evaluasi KAMI (Keamanan Informasi) melalui Manajemen OSSIM (Open Souce SIEM) di UIN Sunan Kalijaga Yogyakarta dapat dilihat pada Gambar 1.



Gambar 1 Alur Penelitian

2.1 Studi Literatur

Tahapan pertama dalam penelitian ini adalah studi literatur untuk mencari referensi dan landasan teori yang digunakan sebagai dasar dalam melakukan penelitian. Studi literatur dilakukan dengan melakukan *review* terhadap jurnal sejenis, membaca berbagai sumber pustaka yang terkait sebagai justifikasi awal untuk melihat apakah ada perbedaan jika ada OSSIM dan tanpa pemasangan OSSIM.

2.2 *Pre-Assesment* Indeks KAMI Jaringan UIN Sunan Kalijaga Yogyakarta

Sebelum melakukan proses simulasi untuk implementasi serangan, dan melihat hasil *network forensic* yang dilakukan, dilakukan paparan mengenai hasil simulasi serangan dan *network forensic* kemudian dilanjutkan pengisian kuesioner *pre-assesment* indeks KAMI kepada responden yang dalam hal ini adalah Kepala Divisi Teknologi Informasi dan pangkalan *data* UIN Sunan Kalijaga Yogyakarta. Hasil kuesioner kemudian dihitung sesuai format *aplikasi* dari Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Indonesia.

2.3 Implementasi Infrastruktur OSSIM jaringan UIN Sunan Kalijaga Yogyakarta

Pada tahapan ini infrasruktur OSSIM diimplementasikan dengan infrastruktur berupa satu buah *server* dan *agent* yang akan ditempatkan dibeberapa titik pada jaringan UIN Sunan Kalijaga Yogyakarta dengan ruang lingkup jaringan yang akan dipantau dibatasi pada jaringan komputer yang berada di UIN Sunan Kalijaga Yogyakarta.

2.4 Monitoring

Tahapan ini dilakukan untuk memantau jaringan untuk mendeteksi usaha penyusupan dengan *Intrusion Detection System*, melakukan proses *filtering*, maupun mendeteksi *Instalation* pada *bandwith* yang tidak wajar pada suatu jaringan sebagai akibat dari serangan pada keamanan jaringan, baik bersifat *internal* maupun *eksternal*.

2.5 *Post-Assesment* Indeks KAMI Jaringan UIN Sunan Kalijaga Yogyakarta

Setelah dilakukan kegiatan pemaparan hasil *monitoring*, dilakukan kembali pengukuran mengenai indeks KAMI terhadap responden yang dalam hal ini adalah Kepala Divisi Teknologi Informasi dan pangkalan *data* UIN Sunan Kalijaga Yogyakarta, dengan memberikan *post-assesment* Indeks Keamanan Informasi (KAMI) untuk mengukur nilai indeks keamanan informasi tersebut setelah dilakukan *monitoring* dengan OSSIM. Hasil kuesioner kemudian dihitung sesuai format aplikasi dari Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Indonesia. Kemudian hasil tersebut akan dibandingkan dengan hasil dari *pre-assesment* yang dilakukan sebelumnya. Apakah ada perbedaan atau tidak, perbedaan tersebut berupa penurunan atau peningkatan dalam indeks KAMI terhadap jaringan sistem di UIN Sunan Kalijaga Yogyakarta.

2.6 Analisis *Data*

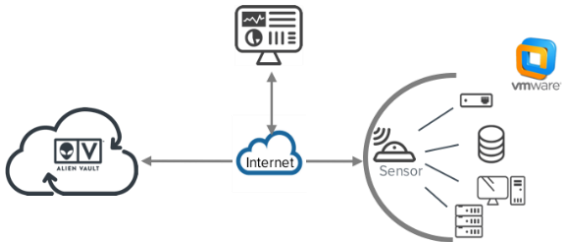
Tahapan akhir ini menganalisis hasil monitoring untuk dibuat perbandingan bagaimana kondisi jaringan sebelum dan sesudah diimplementasikan *Open Souce* SIEM(OSSIM) pada jaringan UIN Sunan Kalijaga Yogyakarta. Hasil dari analisis ini dibuat menjadi kesimpulan untuk menjadi bahan masukan dalam manajemen keamanan jaringan di masa depan.

3. HASIL DAN PEMBAHASAN

3.1 Arsitekstur OSSIM

Arsitekstur dari OSSIM diantaranya sebagai berikut:

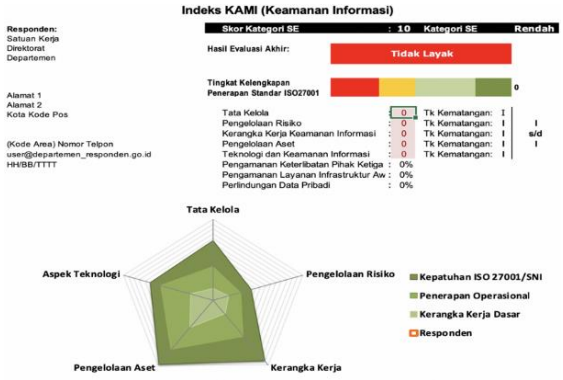
1) *Sensor*, adalah memantau kegiatan-kegiatan suatu sistem jaringan. Segala kejadian pada suatu jaringan atau peristiwa peristiwa yang dapat diterima oleh *server* OSSIM ini menggunakan *sensor*, pada hal ini sensor mampu disebut sebagai pendeteksi.
2) Manajement *server*, adalah pusat dari segala informasi yang diterima dari *sensor-sensor* OSSIM. Adapun fungsi dari Manajemen *Server* ini adalah:
   a. Server utama yang berfungsi untuk memberikan prioritas, menormalisasi, melakukan *risk assesment*, mengkoleksi, dan mengkorelasi perangkat perangkat lainnya.
   b. Melakukan tugas-tugas eksternal dan perawatan seperti *backup scheduled*, *backup data*, mengajukan atau melakukan pens*can*an dan *inventory* secara *online*.
3) *Database*, berfungsi melakukan penyimpanan *data* pada semua kejadian di suatu sistem jaringan sebagai informasi untuk manajemen sistem. Secara umum, Sistem pada OSSIM digambarkan pada Gambar 2 (Hadiansyah chandra and Iskandar, 2017).



Gambar 2 Arsitektur OSSIM

3.2 Alat Evaluasi Indeks KAMI

Alat evaluasi Indeks KAMI dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya yang dijelaskan berdasarkan Gambar 3.



Gambar 3 Grafik Indeks KAMI

Berdasarkan Gambar 3, terkait grafik Indeks KAMI tentang evaluasi yang dilakukan dengan menggunakan indeks Keamanan Informasi (KAMI) ini mencakup 5 target *area*, yaitu:

1) Tata Kelola Keamanan Informasi

Pada bagian ini dilakukan evaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi serta tugas dan tanggung jawab pengelola keamanan informasi. Kontrol yang diperlukan adalah kebijakan formal yang mendefinisikan peran, tanggung jawab, kewenangan pengelolaan keamanan informasi dari pimpinan unit kerja sampai ke pelaksana operasional. Termasuk juga adanya program

kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi.

2) Pengelolaan Risiko Keamanan Informasi

Pada bagian ini dilakukan evaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Kontrol yang diberlakukan adalah adanya kerangka kerja pengelolaan risiko dengan definisi yang eksplisit terkait ambang batas diterimanya risiko, program pengelolaan risiko dan langkah mitigasi yang secara reguler dikaji keefektivitasanny

3) Kerangka Kerja Keamanan Informasi

Pada bagian ini dilakukan evaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Kontrol yang diperlukan adalah sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektivitas kontrol dan langkah perbaikan.

4) Pengelolaan *Asset* informasi

Pada bagian ini dilakukan evaluasi kelengkapan pengamanan terhadap *asset* informasi, termasuk keseluruhan siklus penggunaan *asset* tersebut. Kontrol yang diperlukan adalah bentuk pengamanan terkait keberadaan *asset* informasi serta keseluruhan proses yang bersifat teknis maupun *administratif* dalam siklus penggunaan *asset* tersebut

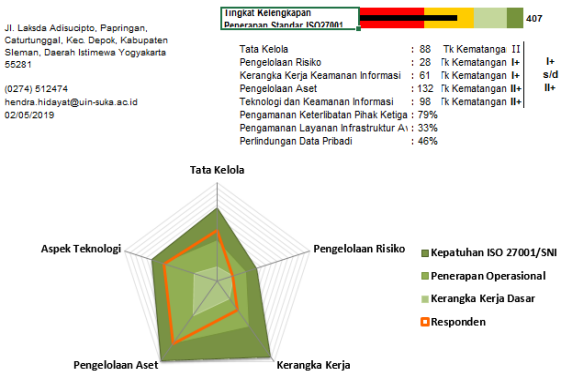
5) Teknologi dan Keamanan Informasi

Pada bagian ini dilakukan evaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan *asset* informasi. Kontrol yang digunakan adalah strategi terkait dengan tingkatan risiko dan tidak secara *eksplisit* menyebutkan teknologi atau merk tertentu.

Dari kelima aspek keamanan informasi berdasarkan indeks Keamanan Informasi (KAMI) maka peran IT dalam mengamankan informasinya dapat terukur dan bisa dijadikan sebagai *input*an kepada pengelola layanan IT.

3.3 Mengkaji Hasil Indeks KAMI

Pada bagian ini akan dijelaskan hasil dari penilaian keseluruhan pada lima *area* keamanan informasi jaringan UIN Sunan Kalijaga Yogyakarta. Berikut dijelaskan *dashboard* pada hasil penilaian lima *area* keamanan informasi di Jaringan UIN Sunan Kalijaga.

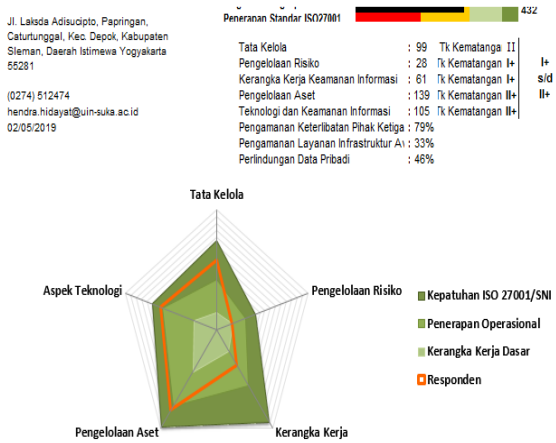


Gambar 4 Dashboard pre-Indeks KAMI

Pada Gambar 4, menunjukan tingkat kategori sistem elektronik yang digunakan oleh jaringan UIN Sunan Kalijaga Yogyakarta berada pada kategori yang Tinggi, dengan nilai 24. Dimana keberlangsungan proses kerja jaringan UIN Sunan Kalijaga Yogyakarta sangat bergantung besar pada penggunaan sistem elektronik. Sementara dari tingkat kelengkapan penerapan standar ISO 27001 berada pada *level* "Pemenuhan Kerangka Kerja Dasar" dengan *level* nilai 407, hal ini menunjukan tingginya ketergantungan instansi terhadap sistem elektronik namun tidak didukung dengan keamanan informasi yang memadai. Dengan hasil evaluasi akhir ini juga menunjukan bahwa jaringan UIN Sunan Kalijaga Yogyakarta membutuhkan perbaikan. Hal ini ditunjukkan dari tingkat kelayakan yang rata-rata menduduki *level* I+ dan II+ sehingga untuk kesiapan sertifikasi masih dikatakan belum layak sertifikasi keamanan informasi, karena untuk mencapai batas minimum kesiapan sertifikasi keamanan informasi adalah tingkat III.

Paparan terhadap hasil analisis forensik jaringan UIN Sunan Kalijaga Yogyakarta dilakukan setelah analisis dan simulasi, kemudian langkah berikutnya melakukan kuesioner ulang sebagai bentuk perbandingan apabila OSSIM di Implementasikan didalam Infrastruktur Jaringan UIN Sunan Kalijaga Yogyakarta. Peneliti melakukan post-assesment terhadap Jaringan UIN Sunan Kalijaga Yogyakarta dengan kuesioner indeks Keamanan Informasi (KAMI) untuk dapat mengukur nilai indeks Keamanan Informasi (KAMI) yang dimiliki oleh instansi tersebut.

Berdasarkan hasil analisis serangan dan korelasinya dengan OSSIM yang dilakukan dan dengan ketergantungan terhadap IT yang tinggi. Terlihat pada gambar 5 menunjukan bahwa nilai dari Jaringan UIN Sunan Kalijaga Yogyakarta adalah 432, yang menunjukan tingkat kelayakan keamanan informasi masih tetap di *level* I+ s/d II+, dan masih di *level* yang sama pada saat *pre-assesment* dilakukan, akan tetapi dari aspek tata kelola, *asset* dan teknologi menunjukan adanya kenaikan *point* nilai dari 407 menuju ke 432.



Gambar 5 Dashboard post-Indeks KAMI

Detail setiap aspek yang ada diukur dalam indeks dapat dilihat di grafik pada Gambar 5, terlihat tidak ada perbedaan untuk aspek management resiko, SOP, pengelolaan *asset*, tetapi terjadi perbedaan pada aspek tata kelola, *asset* dan teknologi yang menunjukan adanya kenaikan sebanyak 10, 7, dan 7 *point* dari *pre-assesment* yang dilakukan .

3.4 Tata kelola Keamanan Informasi

Tabel 1 Nilai Kelayakan Area Tata Kelola Keamanan Informasi (i)

Deskripsi	Hasil
Jumlah pertanyaan Tahap 1	8
Jumlah pertanyaan Tahap 2	8
Jumlah pertanyaan Tahap 3	6
Batas Skor Min untuk Skor Tahap Penerapan 3	48
Total Skor Tahap Penerapan 1 & 2	57
Status Peniliaian Tahap Penerapan 3	*Valid*
Skor Tingkat Kematangan II	41
Skor Minimum Tingkat Kematangan II	*12*
Skor Pencapaian Tingkat Kematangan II	*36*
Status	II
Skor Tingkat Kematangan III	16
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	8
Skor Pencapaian Tingkat Kematangan III	14
Status	No
Skor Tingkat Kematangan IV	42
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	24
Skor Pencapaian Tingkat Kematangan IV	54
Status	No

Tabel 2 Nilai Kelayakan Area Tata Kelola Keamanan Informasi (ii)

***Status* Penerapan**	**Tingkat Kelayakan**				**Total**
	II	**III**	**IV**	**V**	
Tidak Dilakukan	0	0	0	0	0
Dalam Perencanaan	1	0	1	0	2
Dalam Penerapan/Diterapkan Sebagian	11	1	4	0	16
Diterapkan Secara Menyeluruh	1	2	1	0	4
Total	**13**	**3**	**6**	**0**	**22**

Nilai kelengkapan yang didapatkan tata kelola keamanan informasi adalah 88, Berdasarkan Tabel 1, diketahui jumlah pertanyaan pada tahap 1,2 dan 3 berturut-turut adalah 8, 8 dan 6 dengan batas nilai minimal untuk nilai tahap penerapan 3 yaitu 48 dan total nilai tahap penerapan 1 & 2 yaitu 52, sehingga *status* penilaian tahap penerapan 3 ber*status* "*Valid*". Untuk nilai tingkat kelayakan II bernilai 36 dengan nilai minimum yaitu 12 serta nilai pencapaain bernilai 36 sehingga mendapat *status* "II". Selanjutnya untuk nilai tingkat kelayakan III bernilai 16 dengan *validitas* "No" serta nilai minimumnya bernilai 8 dan nilai pencapaain bernilai 14 sehingga mendapat *status* "No". selanjutnya untuk nilai tingkat kelayakan IV bernilai 36 dengan *validitas* "No" serta nilai minimum yaitu 24 dan nilai pencapaain bernilai 54 sehingga mendapat *status* "No".

Berdasarkan Tabel 2, terdapat 2 pertanyaan masing-masing pada tingkat kelayakan II dan IV yang telah direspon "Dalam Perencanaan". Selanjutnya pada *status* penerapan "Dalam Penerapan/Diterapkan Sebagian" terdapat 16 pertanyaan yang telah direspon masing-masing pada tingkat kelayakan II, III, dan IV berturut-turut adalah 11, 1, dan 4. Sedangkan pada *status* penerapan "Diterapkan Secara Menyeluruh" terdapat 4 pertanyaan yang telah direspon pada tingkat II, III dan IV masing-masing berturut-turut adalah 1, 2 dan 1. Berdasarkan hasil yang diperoleh diketahui bahwa pemahaman tentang keamanan informasi cukup besar dalam instansi, pengamanan informasi belum dipetakan lengkap dan terintegrasi, pengidentifikasian *data* pribadi, *metrik* dan *parameter* serta proses pengukuran kinerja masih proses perencanaan dan belum mendefinisikan kebijakan, langkah pidana insiden keamanan informasi dan beberapa masalah tata kelola keamanan informasi.

3.5 Pengelolaan Risiko Keamanan Informasi

Tabel 3 Nilai Kelayakan Area Pengelolaan Risiko Keamanan Informasi (i)

Deskripsi	Hasil
Skor Tingkat Kematangan II	16
Skor Minimum Tingkat Kematangan II	14
Skor Pencapaian Tingkat Kematangan II	20
Status	I+
Skor Tingkat Kematangan III	8
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	4
Skor Pencapaian Tingkat Kematangan III	8
Status	No
Skor Tingkat Kematangan IV	4
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	8
Skor Pencapaian Tingkat Kematangan IV	12
Status	No
Skor Tingkat Kematangan V	0
Validitas Tingkat Kematangan V	No
Skor Minimum Tingkat Kematangan V	12
Skor Pencapaian Tingkat Kematangan V	18
Status	No

Tabel 4 Nilai Kelayakan Area Pengelolaan Risiko Keamanan Informasi (ii)

***Status* Penerapan**	**Tingkat Kelayakan**				**Total**
	II	**III**	**IV**	**V**	
Tidak Dilakukan	0	0	0	0	0
Dalam Perencanaan	4	0	2	2	8
Dalam Penerapan/ Diterapkan Sebagian	6	2	0	0	8
Diterapkan Secara Menyeluruh	0	0	0	0	0
Total	**10**	**2**	**2**	**2**	**16**

Nilai kelengkapan yang didapatkan pengelolaan risiko keamanan informasi adalah 28, Berdasarkan Tabel 3, diketahui jumlah pertanyaan pada tahap 1, 2 dan 3 berturut-turut adalah 10, 4 dan 2 dengan batas nilai minimal untuk nilai tahap penerapan 3 yaitu 36 dan total nilai tahap penerapan 1 & 2 yaitu 28, sehingga *status* penilaian tahap penerapan 3 ber*status* " Tidak *Valid*". Untuk nilai tingkat kelayakan II bernilai 16 dengan nilai minimum yaitu 14 serta nilai pencapaain bernilai 20 sehingga mendapat *status* "I+". Selanjutnya untuk nilai tingkat kelayakan III bernilai 8 dengan *validitas* "No" serta nilai minimumnya bernilai 4 dan nilai pencapaain bernilai 8 sehingga mendapat *status* "No". selanjutnya untuk nilai tingkat kelayakan IV bernilai 4 dengan *validitas* "No" serta nilai minimum yaitu 8 dan nilai pencapaain bernilai 12 dengan *status* "No". selanjutnya untuk nilai tingkat kelayakan V bernilai 0 dengan *validitas* "No" serta nilai minimum yaitu 12 dan nilai pencapaain bernilai 18 sehingga mendapat *status* "No".

Berdasarkan Tabel 4, terdapat 8 pertanyaan pada tingkat kelayakan II, IV dan V yang di respon "Dalam Perencanaan" berturut-turut adalah 4, 2 dan 2. Selanjutnya pada *status* penerapan "Dalam Penerapan/Diterapkan Sebagian" terdapat 8 pertanyaan yang telah direspon masing-masing pada tingkat kelayakan II dan III berturut-turut adalah 6 dan 2. Serta untuk tingkat kelayakan pada *status* penerapan "Diterapkan Secara Menyeluruh" tidak terdapat pertanyaan yang direspon. Berdasarkan hasil tersebut dapat diketahui pengelolaan risiko keamanan informasi sudah diterapkan sebagian, dokumentasi program kerja dan kerangka kerja pengelolaan risiko keamanan informasi belum diterapkan atau masih dalam perencanaan, dan beberapa masalah lain pengelolaan risiko keamanan informasi.

3.6 Kerangka Kerja Pengelolaan Keamanan Informasi

Tabel 5 nilai kelayakan area kerangka kerja keamanan informasi (i)

Deskripsi	Hasil
Jumlah pertanyaan Tahap 1	12
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	7
Batas Skor Min untuk Skor Tahap Penerapan 3	64
Total Skor Tahap Penerapan 1 & 2	61
Status Peniliaian Tahap Penerapan 3	Tidak *Valid*
Skor Tingkat Kematangan II	18
Skor Minimum Tingkat Kematangan II	15
Skor Pencapaian Tingkat Kematangan II	24
Status	I+
Skor Tingkat Kematangan III	43
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	45
Skor Pencapaian Tingkat Kematangan III	62
Status	No
Skor Tingkat Kematangan IV	0
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	15
Skor Pencapaian Tingkat Kematangan IV	27
Status	No
Skor Tingkat Kematangan V	0
Validitas Tingkat Kematangan V	No
Skor Minimum Tingkat Kematangan V	12
Skor Pencapaian Tingkat Kematangan V	18
Status	No

Tabel 6 Nilai Kelayakan Area Kerangka Kerja Keamanan Informasi (ii)

Status Penerapan	Tingkat Kelayakan				Total
	II	III	IV	V	
Tidak Dilakukan	0	0	0	0	0
Dalam Perencanaan	6	0	0	0	6
Dalam Penerapan/Diterapkan Sebagian	5	9	3	2	19
Diterapkan Secara Menyeluruh	0	4	0	0	4
Total	11	13	3	2	29

Nilai kelengkapan yang didapatkan kerangka kerja pengelolaan keamanan informasi adalah 61. Berdasarkan Tabel 5, diketahui jumlah pertanyaan pada tahap 1,2 dan 3 berturut-turut adalah 12, 10 dan 7 dengan batas nilai minimal untuk nilai tahap penerapan 3 yaitu 64 dan total nilai tahap penerapan 1 & 2 yaitu 61, sehingga *status* penilaian tahap penerapan 3 ber*status* " Tidak *Valid*". Untuk nilai tingkat kelayakan II bernilai 18 dengan nilai minimum yaitu 15 serta nilai pencapaain bernilai 24 sehingga mendapat *status* "I+". Selanjutnya untuk nilai tingkat kelayakan III bernilai 43 dengan *validitas* "No" serta nilai minimumnya bernilai 45 dan nilai pencapaain bernilai 62 sehingga mendapat *status* "No". selanjutnya untuk nilai tingkat kelayakan IV bernilai 0 dengan *validitas* "No" serta nilai minimum yaitu 15 dan nilai pencapaain bernilai 27 dengan *status* "No". selanjutnya untuk nilai tingkat kelayakan V bernilai 0 dengan *validitas* "No" serta nilai minimum yaitu 12 dan nilai pencapaain bernilai 18 sehingga mendapat *status* "No".

Berdasarkan Tabel 6, terdapat 6 pertanyaan pada tingkat kelayakan II yang telah direspon "Dalam Perencanaan". Selanjutnya pada *status* penerapan "Dalam Penerapan/Diterapkan Sebagian" terdapat 19 pertanyaan yang telah direspon masing-masing pada tingkat kelayakan II, III, IV dan V berturut-turut adalah 5, 9, 3 dan 2. Sedangkan pada *status* penerapan "Diterapkan Secara Menyeluruh" terdapat 4 pertanyaan pada tingkat kelayakan III. Dari hasil tersebut diketahui bahwa keseluruhan dokumen kebijakan dan prosedur keamanan informasi masih dalam perencanaan, belum terdapat konsekuensi dan

proses tindak lanjut terhadap pelanggaran, instansi belum menerapkan proses pengembangan sistem yang aman (*secure SDLC*), jaringan UIN Sunan Kalijaga Yogyakarta belum memiliki *disaster recovery plan* dikarenakan *server* berpusat pada satu gedung utama dan tidak terdapat *Backup*-an digedung lain serta beberapa masalah kerangka kerja pengelolaan keamanan informasi.

3.7 Pengelolaan *Asset* Informasi

Tabel 7 Nilai Kelayakan *Area* Pengelolaan *Asset* Informasi (i)

Deskripsi	Hasil
Jumlah pertanyaan Tahap 1	24
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	4
Batas Skor Min untuk Skor Tahap Penerapan 3	88
Total Skor Tahap Penerapan 1 & 2	105
Status Peniliaian Tahap Penerapan 3	*Valid*
Skor Tingkat Kematangan II	91
Skor Minimum Tingkat Kematangan II	25
Skor Pencapaian Tingkat Kematangan II	62
Status	II
Skor Tingkat Kematangan III	48
Validitas Tingkat Kematangan III	Yes
Skor Minimum Tingkat Kematangan III	35
Skor Pencapaian Tingkat Kematangan III	50
Status	II+

Tabel 8 Nilai Kelayakan Area Pengelolaan Asset (ii)

Status Penerapan	Tingkat Kelayakan				Total
	II	III	IV	V	
Tidak Dilakukan	0	0	0	0	0
Dalam Perencanaan	0	2	0	0	2
Dalam Penerapan/ Diterapkan Sebagian	14	5	0	0	19
Diterapkan Secara Menyeluruh	15	2	0	0	17
Total	29	9	0	0	38

Nilai kelengkapan yang didapatkan pada pengelolaan *asset* informasi adalah 132. Berdasarkan Tabel 7, diketahui jumlah pertanyaan pada tahap 1,2 dan 3 berturut-turut adalah 24, 10 dan 4 dengan batas nilai minimal untuk nilai tahap penerapan 3 yaitu 88 dan total nilai tahap penerapan 1 & 2 yaitu 98, sehingga *status* penilaian tahap penerapan 3 ber*status* "*Valid*". Untuk nilai tingkat kelayakan II bernilai 86 dengan nilai minimum yaitu 25 serta nilai pencapaian bernilai 62 sehingga mendapat *status* "II". Selanjutnya untuk nilai tingkat kelayakan III bernilai 46 dengan *validitas* "Yes" serta nilai minimumnya bernilai 35 dan nilai pencapaain bernilai 50 sehingga mendapat *status* "II+".

Berdasarkan Tabel 8, terdapat 2 pertanyaan pada tingkat kelayakan III yang telah direspon "Dalam Perencanaan". Selanjutnya pada *status* penerapan "Dalam Penerapan/Diterapkan Sebagian" terdapat 19 pertanyaan yang telah direspon masing-masing pada tingkat kelayakan II dan III berturut-turut adalah 14 dan 5. Sedangkan pada *status* penerapan "Diterapkan Secara Menyeluruh" terdapat 17 pertanyaan yang telah direspon pada tingkat II dan III masing-masing berturut-turut adalah 15 dan 2. Berdasarkan hasil tersebut dapat diketahui jaringan UIN Sunan Kalijaga Yogyakarta sudah mengurus *asset* teknologi informasi cukup baik, dalam proses penerapan mitigasi risiko jaringan UIN Sunan Kalijaga Yogyakarta, belum melakukan ketetapan terkait pertukaran *data* dengan pihak *eksternal* dan pengamanannya, masih merencanakan prosedur penggunaan perangkat pengolah informasi yang dimiliki pihak ketiga serta beberapa masalah pengelolaan *asset* informasi.

3.8 Teknologi dan Keamanan Informasi

Tabel 9 Nilai Kelayakan Area Kerangka Teknologi Dan Keamanan Informasi (i)

Deskripsi	Hasil
Jumlah pertanyaan Tahap 1	14
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	2
Batas Skor Min untuk Skor Tahap Penerapan 3	68
Total Skor Tahap Penerapan 1 & 2	87
Status Peniliaian Tahap Penerapan 3	*Vali d*
Skor Tingkat Kematangan II	39
Skor Minimum Tingkat Kematangan II	18
Skor Pencapaian Tingkat Kematangan II	28
Status	II
Skor Tingkat Kematangan III	57
Validitas Tingkat Kematangan III	Yes
Skor Minimum Tingkat Kematangan III	40
Skor Pencapaian Tingkat Kematangan III	62
Status	II+
Skor Tingkat Kematangan IV	9
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	6
Skor Pencapaian Tingkat Kematangan IV	9
Status	No

Tabel 10 Nilai Kelayakan Area Kerangka Teknologi Dan Keamanan Informasi (ii)

Status Penerapan	Tingkat Kelayakan				Total
	II	III	IV	V	
Tidak Dilakukan	0	0	0	0	0
Dalam Perencanaan	0	1	0	0	1
Dalam Penerapan/ Diterapkan Sebagian	4	3	1	0	8
Diterapkan Secara Menyeluruh	10	5	0	0	15
Total	14	11	1	0	26

Nilai kelengkapan yang didapatkan teknologi dan keamanan informasi adalah 98. Berdasarkan Tabel 9, diketahui jumlah pertanyaan pada tahap 1,2 dan 3 berturut-turut adalah 14, 10 dan 2 dengan batas nilai minimal untuk nilai tahap penerapan 3 yaitu 68 dan total nilai tahap penerapan 1 & 2 yaitu 86, sehingga *status* penilaian tahap penerapan 3 ber*status* " *Valid*". Untuk nilai tingkat kelayakan II bernilai 38 dengan nilai minimum yaitu 18 serta nilai pencapaain bernilai 28 sehingga mendapat *status* "II". Selanjutnya untuk nilai tingkat kelayakan III bernilai 54 dengan *validitas* "Yes" serta nilai minimumnya bernilai 40 dan nilai pencapaain bernilai 62 sehingga mendapat *status* "II+". selanjutnya untuk nilai tingkat kelayakan IV bernilai 6 dengan *validitas* "No" serta

nilai minimum yaitu 6 dan nilai pencapaain bernilai 9 dengan *status* "No".

Berdasarkan Tabel 10 terdapat 1 pertanyaan pada tingkat kelayakan III yang telah direspon "Dalam Perencanaan". Selanjutnya pada *status* penerapan "Dalam Penerapan/Diterapkan Sebagian" terdapat 8 pertanyaan yang telah direspon masing-masing pada tingkat kelayakan II, III dan IV berturut-turut adalah 4, 3 dan 1. Sedangkan pada *status* penerapan "Diterapkan Secara Menyeluruh" terdapat 15 pertanyaan yang telah direspon pada tingkat II dan III masing-masing berturut-turut adalah 10 dan 5. Berdasarkan hasil tersebut dapat diketahui yaitu penggunaan internet pada layanan TIK telah dilindungi pengamanan berlapis, tersedia konfigurasi standar keamanan sistem, adanya standar penggunaan *enskripsi*, instansi memiliki rekaman analisa yang mengkonfirmasi *antivirus/malware* telah dimutakhirkan dan beberapa masalah teknologi dan keamanan informasi lainnya.

Berikut hasil tingkat kelayakan untuk seluruh *area* berdasarkan tingkat *validitas* nilai.

Tabel 11 Hasil Tingkat Kelayakan

	Tata Kelola	**Pengelolaan Risiko**	**Kerangka Kerja**	**Pengelolaan *Asset***	**Aspek Teknologi**
Tingkat II					
Status	II	I+	I+	II	II
Tingkat III					
Validitas	No	No	No	Yes	Yes
Status	No	No	No	II+	II+
Tingkat IV					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Tingkat V					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
***Status* Akhir**	II 3	I+ 2	I+ 2	II+ 4	II+ 4

Berdasarkan Tabel 11 diketahui bahwa *status* kelayakan lima *area* keamanan informasi untuk *status* keamanan informasi berada tingkat II bernilai "II" pada aspek tata kelola, pengelolaan *asset* dan aspek teknologi serta "I+" pada aspek pengelolaan risiko dan aspek kerangka kerja. Hal ini membuktikan bahwa nilai yang didapatkan hampir memenuhi syarat untuk masuk pada *level* kelayakan III. Pada tingkat III untuk aspek pengelolaan *asset* dan aspek teknologi memiliki *validitas* "Yes" dengan *status* "II+" sedangkan pada aspek lain memiliki *validitas* "No". Untuk Tingkat IV dan V masih memiliki *validitas* "No", dapat mencapai tingkat kelayakan III pada syarat indeks KAMI apabila sebagian besar ditingkat kelayakan sebelumnya rumus standar Keamanan Informasi [x-1] dengan indikator sudah "Diterapkan Secara Menyeluruh".Sedangkan sebagai paduan standar ISO/IEC 27001:2005, tingkat kelayakan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah tingkat III+.

Tabel 12 Trafik Protokol TCP

Tanggal	**Jam Kerja**	**Bukan Jam Kerja**
16	98,92 kb/s	218,02 kb/s
17	28,04 kb/s	226,72 kb/s
18	26,95 kb/s	214,57 kb/s
19	58,41 kb/s	202,89 kb/s
20	42,75 kb/s	216,15 kb/s
21	29,68 kb/s	194,01 kb/s
22	36,14 kb/s	196,6 kb/s

Tabel 13 Trafik Protokol UDP

Tanggal	**Jam Kerja**	**Bukan Jam Kerja**
16	32,44 kb/s	13,92 kb/s
17	24,28 kb/s	12,97 kb/s
18	19,81 kb/s	14,95 kb/s
19	22,65 kb/s	13,31 kb/s
20	21,31 kb/s	14,07 kb/s
21	17,05 kb/s	11,52 kb/s
22	18,72 kb/s	14,18 kb/s

Tabel 14 Trafik Protokol ICMP

Tanggal	**Jam Kerja**	**Bukan Jam Kerja**
16	24,62 b/s	33,64 b/s
17	22,41 b/s	30,76 b/s
18	18,62 b/s	24,18 b/s
19	20,52 b/s	25,91 b/s
20	23,68 b/s	28,99 b/s
21	19,61 b/s	30,62 b/s
22	22,58 b/s	32,44 b/s

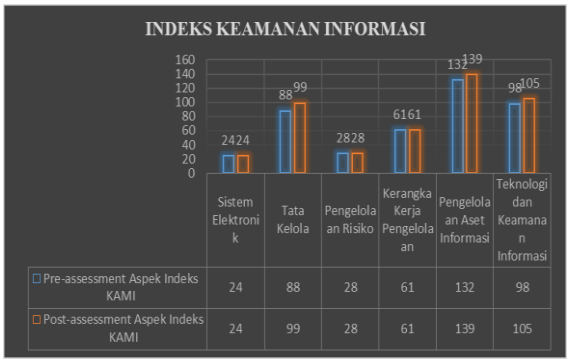
Sistem deteksi berdasarkan *anomali* dengan mengamati aktivitas-aktivitas trafik jaringan yang menyimpang secara *signifikan* dari penggunaan trafik normal. Sistem ini menggangap sesuatu yang tidak normal sebagai anomali. Kontruksi jaringan dari sistem deteksi ini dimulai dengan membangun model kondisi *normal* dan jaringan yang diamati yang kemudian dilanjutkan sebagai kondisi *abnormal.* Kelebihan dari sistem deteksi berdasarkan anomali adalah tidak perlunya pemahaman mendalam tentang *malware* dan dapat mendeteksi serangan berupa *malware* yang baru. Kekurangannya adalah tidak dapat diketahui tipe serangan apa yang menyerang jaringan. *Open Souce SIEM*(OSSIM) memiliki kemampuan untuk melakukan pengamatan trafik jaringan seperti pengamatan trafik protokol. Pada penelitian ini langkah selanjutnya adalah melakukan monitoring dan pengambilan *data* trafik protokol pada sistem jaringan di UIN Sunan Kalijaga Yogyakarta. selama satu minggu dari tanggal 16 September 2019 sampai tanggal 22 September 2019 dan pengamatan dilakukan pada jam kerja pad pukul 08.00- 16.00 dan bukan jam kerja pada pukul 16.00-08.00 . Adapun *data* yang diambil adalah nilai rata-rata dari protokol TCP, UDP dan ICMP. *Data* hasil pengamatan trafik TCP, UDP dan ICMP bisa di lihat pada Tabel 12, Tabel 13 dan Tabel 14.

Tujuan pengambilan *data* ini adalah untuk menganalisa kondisi keamanan dan jaringan, dengan cara memonitoring perubahan trafik jaringan. Dari *data* pengamatan didapatkan bahwa kondisi jaringan dari ketiga protokol saat jam kerja lebih kecil dibandingkan dengan Bukan Jam kerja.

Tabel 15 Rata-rata Trafik Protokol

Protokol	Jam Kerja	Bukan Jam Kerja	Selisih
TCP	45,84 kb/s	209,85 kb/s	164,01
UDP	22,32 kb/s	13,56 kb/s	8,76
ICMP	21,72 b/s	29,49 b/s	7,77

Dari *data* yang ada pada Tabel 15 dapat diambil kesimpulan bahwa rata-rata trafik TCP lebih besar 164,01 kb/s pada saat bukan jam kerja, rata-rata trafik UDP lebih besar 8,76 kb/s pada saat jam kerja dan rata-rata ICMP lebih besar 9,63 b/s pada saat bukan jam kerja.



Gambar 6 Nilai indeks (KAMI) *Pre-Assessment* dan *Post-Assessment* Jaringan UIN Sunan Kalijaga Yogyakarta

Berdasarkan Gambar 6, penyebab kenaikan nilai indeks Keamanan Informasi (KAMI) dari beberapa aspek tata kelola, pengelolaan *asset* informasi dan teknologi keamanan informasi yang dipengaruhi oleh beberapa *point* yang ditunjukan pada Tabel 16, Tabel 17, Tabel 18, Tabel 19, Tabel 20, Tabel 21.

Tabel 16 Aspek "Tata kelola Keamanan Informasi" Pre-Assesment

No	Evaluasi Tata Kelola Keamanan Informasi	*Status*	*Point*
1	Apakah instansi/perusahaan pada jaringan Keamanan Informasi di UIN Sunan Kalijaga Yogyakarta sudah menerapkan peningkatan pemahaman dan program sosialisasi untuk keamanan informasi,termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Penerapan/ Diterapkan Sebagian	2
2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Penerapan/ Diterapkan Sebagian	4
3	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Dalam Penerapan/ Diterapkan Sebagian	4
4	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Dalam Penerapan/ Diterapkan Sebagian	6
5	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Penerapan/ Diterapkan Sebagian	6

Tabel 17 Aspek "Tata kelola Keamanan Informasi" post-assesment

No	Evaluasi Tata Kelola Keamanan Informasi	*Status*	*Point*
1	Apakah jaringan UIN Sunan Kalijaga Yogyakarta sudah menerapkan peningkatan pemahaman dan program sosialisasi untuk keamanan informasi, termasuk kepentingan tingkat ketaatan bagi semua pihak yang terkait?	Diterapkan Secara Menyeluruh	3
2	Apakah jaringan UIN Sunan Kalijaga Yogyakarta anda menerapkan program keahlian dan peningkatan kompetensi untuk petugas dan pejabat pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	6
3	Apakah jaringan UIN Sunan Kalijaga Yogyakarta anda sudah mengintegrasikan persyaratan/ keperluan keamanan informasi pada proses kerja yang ada?	Diterapkan Secara Menyeluruh	6
4	Apakah jaringan UIN Sunan Kalijaga Yogyakarta anda sudah mendefinisikan proses, metrik, dan parameter pada pengukuran kinerja pengelolaan keamanan informasi yang mencakup waktu, pengukuran, waktu mekanisme, pemantauannya, pelaporannya, dan eskalasi pelaksananya?	Diterapkan Secara Menyeluruh	9
5	Apakah jaringan UIN Sunan Kalijaga Yogyakarta anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (petugas dan pejabat) pelaksananya?	Diterapkan Secara Menyeluruh	9

Tabel 18 Aspek "Pengelolaan *Asset* Informasi" *Pre-Assesment*

No	Evaluasi Pengelolaan *Asset* Informasi	*Status*	*Point*
1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Dalam Penerapan/ Diterapkan Sebagian	2
2	Prosedur penghancuran *data*/*asset* yang sudah tidak diperlukan	Dalam Perencanaan	2
3	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan *asset* informasi penting?	Dalam Penerapan/ Diterapkan Sebagian	4

No	Evaluasi Pengelolaan *Asset* Informasi	*Status*	*Point*
4	Apakah tersedia mekanisme pengamanan dalam pengiriman *asset* informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Penerapan/ Diterapkan Sebagian	4

Tabel 19 Aspek "Pengelolaan Asset Informasi" Post-Assesment

No	Evaluasi Pengelolaan *Asset* Informasi	*Status*	*Point*
1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Diterapkan Secara Menyeluruh	3
2	Prosedur penghancuran *data*/*asset* yang sudah tidak diperlukan	Dalam Perencanaan	2
3	Apakah tersedia proses pada jaringan UIN Sunan Kalijaga Yogyakarta untuk merawat perangkat computer, kelayakan keamanan lokasi kerja , memeriksa (inspeksi), fasilitas pendukungnya untuk menempatkan *asset* informasi yang penting?	Diterapkan Secara Menyeluruh	6
4	Apakah tersedia mekanisme pada jaringan UIN Sunan Kalijaga, pengamanan pada pengiriman *asset* informasi (dokumen dan perangkat) yang melibatkan pihak ketiga?	Diterapkan Secara Menyeluruh	6

Tabel 20 Aspek "Teknologi dan Keamanan Informasi" Pre-Assesment

No	Evaluasi Teknologi dan Keamanan Informasi	*Status*	*Point*
1	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?	Dalam Penerapan/ Diterapkan Sebagian	2
2	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Dalam Penerapan/ Diterapkan Sebagian	6
3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Dalam Penerapan/ Diterapkan Sebagian	6

Tabel 21 Aspek "Teknologi dan Keamanan Informasi" Post-Assesment

No	Evaluasi Teknologi dan Keamanan Informasi	*Status*	*Point*
1	Apakah sistem operasi untuk setiap perangkat desktop dan server hirkan dengan versi terkini?	Diterapkan Secara Menyeluruh	3
2	Apakah jaringan pada UIN Sunan Kalijaga Yogyakarta anda menerapkan uji coba dan lingkungan pengembangan yang sudah diamankan sesuai dengan digunakan untuk seluruh siklus hidup sistem yng dibangun dan standar platform teknologi yang ada?	Diterapkan Secara Menyeluruh	9
3	Apakah jaringan UIN Sunan Kalijaga anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Diterapkan Secara Menyeluruh	9

Hasil perbandingan diatas yang merupakan hasil dari kuesioner tersebut, kemudian dihitung sesuai dengan format aplikasi yang dimiliki oleh Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Indonesia dan menujukan bahwa penggunaan *Open Souce SIEM*(OSSIM) dapat membantu menaikan nilai *point* untuk aspek Teknologi yang ada pada indeks Keamanan Informasi (KAMI) akan tetapi tidak berpengaruh pada aspek-aspek yang lain. Terlihat bahwa nilai dari Jaringan UIN Sunan Kalijaga Yogyakarta adalah 432 pada Gambar 5, dari sebelummnya adalah 407 *point* pada Gambar 4, yang menunjukan tingkat kelayakan keamanan informasi masih di I+ s/d II+, masih di *level* yang sama pada saat *pre-assesment* dilakukan, akan tetapi dari aspek tata kelola menunjukan adanya perubahan nilai dari 88 menuju ke 99, pengelolaan *asset* menunjukan adanya perubahan nilai dari 132 menuju ke 139, dan teknologi menunjukan adanya perubahan nilai dari 98 menuju ke 105 yang dijelaskan pada Gambar 6. Dengan memonitor kondisi jaringan UIN Sunan Kalijaga Yogyakarta dapat diperoleh tujuan dari penelitian ini, yakni memantau dan mengetahui lebih detail permasalahan yang ada pada Jaringan UIN Sunan Kalijaga Yogyakarta sehingga dapat diketahui pola solusi untuk mengatasinya sehingga dapat memaksimalkan infrastruktur jaringan komputer yang ada dengan lebih efektif dan efisien sesuai fungsinya sebagai institusi pendidikan.

4. KESIMPULAN

Data indeks Keamanan Informasi (KAMI) didapatkan melalui pengisian kuesioner mengenai *Evaluasi* Manajemen Keamanan Informasi pada Jaringan UIN Sunan Kalijaga Yogyakarta selanjutnya hasil kuesioner baru dibandingkan dengan hasil kuesioner sebelumnya. Berdasarkan tingkat kelengkapan dan kelayakan nilai indeks KAMI yang diujikan pada jaringan UIN Sunan Kalijaga Yogyakarta masih rendah. Penyebab rendahnya tingkat kelengkapan dan kelayakan keamanan informasi ini adalah jaringan UIN Sunan Kalijaga Yogyakarta belum menerapkan semua syarat keamanan informasi atau masih dalam perencanaan. Dalam hubungannya dengan indeks KAMI pengunaan teknologi *Open Source SIEM* (OSSIM) terbukti dapat menaikan nilai indeks KAMI Jaringan

UIN Sunan Kalijaga Yogyakarta pada berbagai aspek, adapun kenaikan ini karena kemampuan OSSIM dalam menganalisa kelemahan dan perubahan konfigurasi *asset* informasi di jaringan UIN Sunan Kalijaga Yogyakarta sekaligus memonitor dan melakukan proses analisa dan *audit* terhadap *asset* yang dimiliki Jaringan UIN Sunan Kalijaga Yogyakarta secara rutin dan sistematis. namun tingkat kelayakan keamanan informasi masih di *level* I+ sampai dengan II+ Sehingga keamanan informasi pada jaringan tidak layak dan butuh perbaikan.

DAFTAR PUSTAKA

AKHIRINA, T. Y., ARIF, S. M. AND AND RAHMATIKA (2016) 'Evaluasi Keamanan Teknologi Informasi pada PT INDOTAMA PARTNER LOGISTICS Menggunakan Indeks Keamanan Informasi (KAMI)', *Jurnal Nasional Teknologi dan Sistem Informasi*, 2(2), pp. 53–62. doi:https://doi.org/10.25077/TEKNOSI.v2i2.2016.53-62.

ANGGA JUANSYAH, BAGUS PRATAMA, I. D. (2018) 'Analisis dan implementasi open source security information managament (ossim) pada keamanan jaringan komputer pt. satria antaran prima palembang'. Available at: http://library.palcomtech.com/pdf/5621.pdf.

BASYARAHIL, F. A., ASTUTI, H. M. AND HIDAYANTO, B. C. (2017) 'Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi (DPTSI) ITS Surabaya', *Jurnal Teknik ITS*, 6(1), p. 227. doi: 10.1016/j.juro.2016.01.039.

HADIANSYAH CHANDRA AND ISKANDAR, I. (2017) 'Pembangunan Server Security Information Management Untuk Monitoring Keamanan Di Server Diskominfo Provinsi Jawa Barat', pp. 1–8. Available at: https://repository.unikom.ac.id/53479/.

HIDAYAT, R., SUYANTO, M. AND SUNYOTO, A. (2018) 'Indeks Penilaian Keamanan Informasi Untuk Mengukur Kematangan Manajemen Keamanan Layanan TI', *Pengembangan Aplikasi Untuk Mendeteksi Pergerakan Sendi Pada Pasien Pasca Stroke Menggunakan Sensor Accelerometer Di Smartphone Android*, 3(1), pp. 1–7.Available at: http://e-journal.janabadra.ac.id/index.php/informasiinteraktif/article/view/671.

ISO/IEC (2018) 'INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and', 2018, p. 38. doi: 10.1177/0011128708322943.

LENAWATI, M., WINARNO, W. W. AND AMBOROWATI, A. (2017) 'Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 Dan COBIT 5', *Sentra Penelitian Engineering dan Edukasi*, 9(1), pp. 44–49. doi: http://dx.doi.org/10.3112/speed.v9i1.1452.

MENKOMINFO (2019) 'Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 8 Tahun 2019', 8(8), pp. 1–48. doi: 10.1017/CBO9781107415324.004.

PRATAMA, E. R., SUPRAPTO AND PERDANAKUSUMA, A. R. (2018) 'Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur', *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2(11), pp. 5911–5920. Available at: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465.

PUTRA, M. Y. AND TJAHJADI, D. (2018) 'Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001', *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, 6(1), pp. 95–104. doi: https://doi.org/10.33558/piksel.v6i1.1404.

SUGIANTORO, B. (2017) 'Pengembangan Deteksi Penyusupan Menggunakan Multiagent', *Telematika*, 14(2), pp. 83–88. doi: https://doi.org/10.31315/telematika.v14i2.2095.

SUTARA, B. (2018) 'Pengukuran Keamanan Informasi PDAM Titra Medal Menggunakan Indeks KAMI Untuk Analisis Tingkat Kematangan Keamanan Informasi', 17(2), pp. 34–41. doi: https://doi.org/10.36054/jict-ikmi.v17i2.32.