

**OPTIMASI KEAMANAN INFORMASI DENGAN
SECURITY INFORMATION AND EVENT
MANAGEMENT (SIEM) MANAGEENGINE
OPMANAGER
(STUDI KASUS: IBISA PURWOREJO)**



Oleh:

Eko JhonyPranata

NIM: 19206050014

**STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA**

**PROGRAM STUDI MAGISTER INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
PASCASARJANA**

**UNIVERSITAS ISLAM NEGERI SUNANKALIJAGA
YOGYAKARTA**

2022

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Eko Jhony Pranata

NIM : 19206050014

Jenjang : Magister

Program Studi : Informatika

Menyatakan bahwasanya naskah tesis dengan judul “Optimasi Keamanan Informasi dengan Security Information and Event Management (SIEM) *ManageEngine OpManager* (Studi Kasus: IBISA purworejo)” tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar magister di suatu Perguruan Tinggi, dan sepengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 22 Agustus 2022

Saya yang menyatakan,

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA



Eko Jhony Pranata

NIM:19206050014

PERNYATAAN BEBAS PLAGIASI

Yang bertanda tangan di bawah ini:

Nama : Eko Jhony Pranata

NIM : 19206050014

Jenjang : Magister

Program Studi : Informatika

Menyatakan bahwa naskah tesis ini secara keseluruhan adalah benar-benar bebas dari plagiasi. Jika di kemudian hari terbukti melakukan plagiasi, maka saya siap ditindak sesuai dengan ketentuan hukum yang berlaku.

Yogyakarta, 22 Agustus 2022

Saya yang menyatakan,



Eko Jhony Pranata

NIM:19206050014

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

PENGESAHAN TUGAS AKHIR



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1791/Un.02/DST/PP.00.9/08/2022

Tugas Akhir dengan judul : OPTIMASI KEAMANAN INFORMASI DENGAN SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MANAGE ENGINE OPMANAGER (STUDI KASUS: IBISA PURWOREJO)

yang dipersiapkan dan disusun oleh:

Nama : EKO JHONY PRANATA, S.Kom
Nomor Induk Mahasiswa : 19206050014
Telah ditujikan pada : Selasa, 09 Agustus 2022
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR



Valid ID: 62f6a7c9a0f

Ketua Sidang

Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D.

SIGNED



Valid ID: 62b003ce9989

Penguji I

Dr. Ir. Shofwatul Uyun, S.T., M.Kom.

SIGNED



Valid ID: 62f9a7a512367

Penguji II

Dr. Ir. Bambang Sugiantoro, S.Si., M.T.

SIGNED



Valid ID: 628f1b17a470b

Yogyakarta, 09 Agustus 2022

UIN Sunan Kalijaga

Dekan Fakultas Sains dan Teknologi

Dr. Dra. Hj. Khurul Wardati, M.Si.

SIGNED

NOTA DINAS PEMBIMBING

Kepada Yth.,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta

Assalamu'alaikum wr. wb.

Setelah melakukan bimbingan, arahan dan koreksi terhadap penulis tesis yang berjudul:
“Optimasi Keamanan Informasi dengan Security Information and Event Management (SIEM) ManageEngine OpManager (Studi Kasus: IBISA purworejo)”

Yang ditulis oleh:

Nama : Eko Jhony Pranata

NIM : 19206050014

Jenjang : Magister

Program Studi : Informatika

Saya berpendapat bahwa tesis tersebut sudah dapat diajukan kepada Magister Informatika UIN Sunan Kalijaga untuk diujikan dalam rangka memperoleh gelar Magister Informatika.

Wassalamu'alaikum wr. wb.

Yogyakarta, 22 Agustus 2022

Pembimbing

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA



(Ir. M Taufiq Nuruzzaman, S.T. M.Eng., Ph.D.)

ABSTRAK

Serangan yang terjadi pada jaringan sudah sangatlah umum untuk saat ini, dengan Semakin banyaknya cara untuk mengakses data dan tentu saja semakin banyak teknologi yang digunakan untuk meningkatkan ancaman terhadap keamanan jaringan. Pemerintah sebagai Regulator menerbitkan Sistem Manajemen Keamanan Informasi (SMKI) dan Indeks Keamanan Informasi (KAMI) Sebagai langkah pengamanan informasi bagi institusi daerah maupun instansi. *Security Information and Event Management (SIEM)* adalah teknologi keamanan untuk melindungi aset informasi. Dalam hal ini *SIEM* dengan menggunakan *ManageEngine OpManager* diharapkan dapat memberikan Optimasi untuk mendukung proses Keamanan Informasi agar dapat menaikkan nilai dari standar Indeks KAMI pada jaringan IBISA. Metode penelitian yang dilakukan meliputi studi literatur, kemudian melakukan Pra-Assessment indeks KAMI, setelah itu melakukan implementasi infrastruktur *ManageEngine OpManager*, kemudian melakukan monitoring terhadap Indeks Keamanan Informasi menggunakan teknologi pada *ManageEngine OpManager*, dan melakukan Post-Assessment Indeks KAMI, selanjutnya tahap akhir ini adalah melakukan Analisis terhadap hasil monitoring dan melakukan perbandingan dari hasil monitoring bagaimana Kondisi jaringan sebelum dan sesudah dilakukannya implementasi *ManageEngine OpManager*. Didapatkan bahwa penggunaan *SIEM* dengan menggunakan *ManageEngine OpManager* untuk melakukan *monitoring* terbukti dapat meningkatkan nilai dari Indeks KAMI pada Aspek Teknologi dan Keamanan Informasi. Selain dari pada itu didapatkan juga kenaikan pada aspek Tata Kelola, Pengelolaan Aset.

Dari hasil evaluasi yang telah didapatkan menunjukkan bahwa jaringan IBISA Purworejo perlu adanya peningkatan dan juga perbaikan. di mana Hasilnya sesuai dengan data aktual dan dapat digunakan untuk membantu perbaikan pada jaringan IBISA Purworejo Berdasarkan Indeks KAMI. Dan juga implementasi Indeks KAMI menggunakan *ManageEngine OpManager* yang telah terbukti Meningkatkan nilai indeks keamanan informasi (KAMI) jaringan IBISA Purworejo dalam berbagai aspek, adapun peningkatan ini karena Kemampuan *ManageEngine OpManager* untuk menganalisis kelemahan dan perubahan Alokasi Aset Informasi di Jaringan IBISA Purworejo.

Kata Kunci: *SIEM*, Indeks KAMI, Keamanan Informasi, *ManageEngine OpManager*

ABSTRACT

Attacks that occur on networks are very common nowadays, with more and more ways to access data and of course more and more technologies are used to increase threats to network security. The government as a regulator publishes the Information Security Management System (SMKI) and the Information Security Index (KAMI) as information security measures for regional institutions and agencies. *Security Information and Event Management* (SIEM) is a security technology to protect information assets. In this case, SIEM using *ManageEngine OpManager* is expected to provide optimization to support the Information Security process in order to increase the value of the KAMI Index standard on the IBISA network. The research method includes a literature study, then pre-Assessment of the US index, after that implementing the *ManageEngine OpManager* infrastructure, then monitoring the Information Security Index using technology on *ManageEngine OpManager*, and conducting Post-Assessment of the KAMI Index, then this final stage is Analyze the monitoring results and compare the results of monitoring the network conditions before and after the implementation of *ManageEngine OpManager*. It was found that the use of SIEM by using *ManageEngine OpManager* for monitoring has been proven to increase the value of the KAMI Index on Information Technology and Security Aspects. Apart from that, there was also an increase in aspects of Governance, Asset Management.

From the evaluation results that have been obtained, it shows that the Purworejo IBISA network needs improvements and also improvements. where the results are in accordance with the actual data and can be used to help improve the Purworejo IBISA network Based on the KAMI Index. And also, the implementation of the KAMI Index *using ManageEngine OpManager* which has been proven to increase the value of the information security index (KAMI) of the IBISA Purworejo network in various aspects, while this increase is due to the ability of *ManageEngine OpManager* to analyze weaknesses and changes in Information Asset Allocation in the IBISA Purworejo Network.

Keywords: *SIEM*, KAMI Index, Information Security, *ManageEngine OpManager*

KATA PENGANTAR



Puji Syukur kehadiran Allah SWT yang telah memberikan rahmat serta hidayah-Nya, sehingga penyusun masih dapat merasakan segala nikmat dan juga kesempatan yang diberikan dalam menyelesaikan tesis yang berjudul **“OPTIMASI KEAMANAN INFORMASI DENGAN SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MANAGEENGINE OPMANAGER (STUDI KASUS : IBISA PURWOREJO)”** Sholawat serta salam semoga senantiasa tetap tercurahkan kepada Nabiullah Nabi besar Muhammad SAW, semoga kita sebagai umatnya mendapat *syafa'at* darinya kelak di hari akhir. Tugas Akhir Tesis ini disusun untuk memenuhi sebagian persyaratan guna mendapatkan gelar Magister Informatika Pada Program Studi Informatika (S2) Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Dalam kesempatan ini penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr.Phil. Al Makin, S.Ag., M.A. selaku Rektor UIN Sunan Kalijaga Yogyakarta
2. Ibu Dr. Dra. Hj. Khurul Wardati, M.Si. selaku Dekan Fakultas Sains dan Teknologi
3. Bapak Dr. Bambang Sugiantoro, S.Si., M.T., dan Ibu Maria Ulfah Siregar, S.Kom. MIT., Ph.D., sebagai Kepala dan

Sekretaris Program Studi Informatika Program Magister
Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta,

4. Bapak Dr. Ir. Shofwatul 'Uyun, S.T., M.Kom. selaku Dosen Pembimbing Akademik Magister Informatika 2019.
5. Bapak Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D. selaku Dosen Pembimbing Tesis yang dengan sabar telah meluangkan waktunya untuk membimbing serta memberikan koreksi dan saran kepada penulis dalam menyelesaikan penelitian Tesis ini.
6. Bapak dan Ibu dosen Program Studi Magister Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta yang telah memberikan ilmu dan pengalaman kepada penulis selama masa kuliah.
7. Seluruh Staff Bagian Kemahasiswaan Sains dan Teknologi, PTIPD UIN Sunan Kalijaga yang telah membantu dalam menyelesaikan Penelitian ini.
8. Ibu Nurma Ika Zuliyanti, SST.M.Kes. Selaku Rektor kampus Institut Teknologi Bisnis dan Kesehatan Bhakti Putra Bangsa Indonesia (IBISA Purworejo)
9. Bapak Hasan Yudi selaku kepala Pusat Data, TI dan Informasi (PUSDATIN) kampus Institut Teknologi Bisnis dan Kesehatan Bhakti Putra Bangsa Indonesia (IBISA Purworejo) beserta staff yang terlibat dalam penyelesaian penelitian ini.

10. Teman-teman seperjuangan Program Studi Magister Informatika 2019 yang telah memberi dukungan dan bantuan dalam penelitian ini.

11. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah membantu dalam proses penyelesaian tesis ini.

Penulis menyadari masih banyak kekurangan dan kelemahan dalam pelaksanaan dan penyusunan tesis ini. Oleh karena itu kritik dan saran penulis harapkan untuk dapat menyempurnakannya. Semoga tesis ini dapat bermanfaat bagi pembaca dan penulis khususnya.

Yogyakarta, 22 Agustus 2022

Penyusun,

Eko Jhony Pranata
NIM:19206050014



STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

HALAMAN PERSEMBAHAN

Alhamdulillah, segala puji Allah SWT dengan kemurahan dan ridho-Nya, Tesis ini dapat ditulis dengan baik dan lancar hingga selesai. Tak lupa sholawat beserta salam kepada tauladan Nabi besar Muhammad SAW sebagai panutan umat muslim yang penuh dengan kemuliaan dan ketaatan kepada Allah SWT memberi ku motivasi tentang kehidupan dan mengajari ku hidup melalui sunnah-sunnah nya. Halaman ini saya tujukan terhadap semua pihak yang telah membantu dan Men support Penyelesaian Tesis ini, dengan ini akan saya persembahkan kepada:

1. Kedua Orang Tua Tercinta, Ibunda Latifah dan Ayahanda Badri serta adikku Dicko Sanjaya dan Dicky Sanjaya serta seluruh anggota keluarga tercinta, yang selalu memberikan nasihat, dukungan, motivasi dan do'anya. "Allaahummaghfirlii dzunubi waliwaalidayya warham humma kamaa rabbayaa nii shaghiiraa."
2. Terima kasih banyak untuk bapak Pembimbing saya Bapak Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D., yang telah membimbing saya dalam pembuatan tesis ini.
3. Segenap Dosen Teknik Informatika dan Magister Informatika UIN Sunan Kalijaga Yogyakarta, Pak Bambang, Pak Agung, Pak Sumarsono, Pak Didik, Pak Nurochman, Pak Agus, Pak Mustaqim, Pak Aulia, Pak Imam, Pak Awik, Bu Uyun, Bu Maria, Bu 5Ade, terima kasih atas ilmu yang telah diberikan selama menempuh perkuliahan, semoga bermanfaat di kemudian hari.

4. Aminatuz Zuhriyyah S.Pd., yang telah memberikan saran, bantuan dan semangat selama proses pengerjaan Tesis. Terima kasih atas ke-riwilannya, kesabaran menghadapi penulis dalam menyelesaikan tiap bait-bait tesis ini.
5. Teman-teman Seperjuangan, keluarga besar Magister Informatika Angkatan 2019 yang tidak bisa saya sebutkan satu persatu, terima kasih untuk kebersamaanya dan dukungan kalian setiap perjuangan kita sebagai mahasiswa Magister Informatika di UIN Sunan Kalijaga Yogyakarta.
6. Keluarga Besar Teknik Informatika Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta
7. Keluarga Besar Magister Informatika Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
8. Ibu Nurma Ika Zuliyanti, SST.M.Kes. Selaku pimpinan kampus Institut Teknologi Bisnis dan Kesehatan Bhakti Putra Bangsa Indonesia (IBISA Purworejo) yang telah memberikan izin penelitian tesis ini.
12. Pak Hasan Yudi selaku kepala Pusat Data, TI dan Informasi (PUSDATIN) kampus Institut Teknologi Bisnis dan Kesehatan Bhakti Putra Bangsa Indonesia (IBISA Purworejo) beserta staff yang terlibat dalam penyelesaian penelitian ini.
9. Konco-konco Seperjuangan OTW jadi Bos (Rizki, Maulana, Setyo, Yuha, Yudi, Asep, Anggoro, Zahid, Roni, Aji Wahyu, Taufik, Tulus, Alviyan) yang telah menemani setiap jejak langkah perjuangan saya selama menuntut ilmu di Yogyakarta, terima kasih untuk canda tawa, menyemangati saya dalam

mengerjakan tesis ini serta tidak lupa lengkap dengan misuh-misuhnya.

10. HJM Racing, Purnomo Motor Sport dan Issabela Racing yang telah menjadi support, menjadi tempat keluh kesah dan juga memberi motivasi serta tempat mencari inspirasi pembuatan kata demi kata selama pengerjaan Tesis ini hingga selesai.
11. Kupersembahkan pula tesis ini untuk orang yang bertanya “kapan tesismu selesai...?? Kok kuliahnya ga slesai-slesai..??
^ ^”
—
12. Saya sangat berterima kasih kepada semua pihak yang telah membantu saya dalam menyelesaikan Tesis ini. Terima kasih telah menyadarkan saya bahwasanya ada tanggung jawab saya untuk menyelesaikan tesis ini, meskipun ada beberapa hal yang tidak kalah pentingnya juga untuk diselesaikan juga, dan terima kasih kepada teman-teman saya yang bersedia meluangkan waktu bersama saya meskipun mempunyai kesibukan masing-masing untuk meyakinkan saya bahwa cepat atau lambat semuanya akan sesuai jadwal Untuk memiliki akhir yang Bahagia, Tuhan adalah sutradara terbaik yang membuat saya mengerti bahwa hidup adalah perjalanan yang memang harus dilalui dan di selesaikan dengan baik meskipun banyak sekali godaan dan cobaan yang menghampiri, bahkan ngantuk dan malas yang luar biasa melanda selama pengerjaan tesis ini.

Demikian halaman persembahan ini saya buat sebagai apresiasi terhadap semua pihak yang telah memberi bantuan baik dari doa, moral, dan material dalam penunjang tesis sini. Terima kasih banyak

tak kurang saya ucapkan dan mohon maaf apabila ada kesalahan dalam penulisan, kurang dan lebihnya mohon dimaafkan.



MOTTO

أَمْ حَسِبْتُمْ أَنْ تُدْخَلُوا الْجَنَّةَ وَلَمَّا يَأْتِكُمْ مَثَلُ الَّذِينَ خَلَوْا مِنْ قَبْلِكُمْ مَسَّتْهُمُ
الْبَأْسَاءُ وَالضَّرَّاءُ وَزُلْزِلُوا حَتَّى يَقُولَ الرَّسُولُ وَالَّذِينَ آمَنُوا مَعَهُ مَتَى نَصْرُ
اللَّهِ ۗ أَلَا إِنَّ نَصْرَ اللَّهِ قَرِيبٌ

“Apakah kamu mengira bahwa kamu akan masuk surga, padahal belum datang kepadamu (cobaan) sebagaimana halnya orang-orang terdahulu sebelum kamu? Mereka ditimpa oleh malapetaka dan kesengsaraan, serta digoncangkan (dengan bermacam-macam cobaan) sehingga berkatalah Rasul dan orang-orang yang beriman bersamanya: "Blakalah datangnya pertolongan Allah?" Ingatlah, sesungguhnya pertolongan Allah itu amat dekat.” (Qs Al-Baqarah:214)

فَإِنَّ مَعَ الْعُسْرِ يُسْرًا إِنَّ مَعَ الْعُسْرِ يُسْرًا

“Karena sesungguhnya sesudah kesulitan itu ada kemudahan. Sesungguhnya sesudah kesulitan itu ada kemudahan.” (Qs Al-Inshirah:5-

6)

“Angin tidak berhembus untuk menggoyangkan pepohonan, melainkan menguji kekuatan akarnya.”

(Ali bin Abi Thalib)

“Pengetahuan yang baik adalah yang memberikan manfaat, bukan hanya diingat.”

(Imam Syafi’i)

“Menuntut ilmu adalah takwa. Menyampaikan ilmu adalah ibadah. Mengulang-ulang ilmu adalah zikir. Mencari ilmu adalah jihad”

(Abu Hamid Al Ghazali)



STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR ISI

COVER	i
PERNYATAAN KEASLIAN	ii
PERNYATAAN BEBAS PLAGIASI	iii
PENGESAHAN TUGAS AKHIR	iv
NOTA DINAS PEMBIMBING	v
ABSTRAK	vi
ABSTRACT	vii
HALAMAN PERSEMBAHAN	xi
MOTTO	xv
DAFTAR ISI	xvii
DAFTAR GAMBAR	xx
DAFTAR TABEL	xxi
DAFTAR SINGKATAN	xxiii
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	5
C. Batasan Masalah	5
D. Tujuan Penelitian	6
E. Manfaat Penelitian	7
F. Keaslian Penelitian	8
G. Sistematika Penulisan	8
BAB II KAJIAN PUSTAKA DAN LANDASAN TEORI	10
A. Kajian Pustaka	10
B. Landasan Teori	42

1. Jaringan	42
3. Router.....	45
4. Mikrotik	48
5. Hotspot	49
6. Information Security.....	49
7. Network Monitoring	53
8. Intrusion Detection System	56
9. Ntop	60
10. SNORT	64
11. GNS3.....	67
12. TCP/IP	68
13. UDP.....	70
14. ICMP	71
15. ManageEngine OpManager	72
16. Indeks Keamanan Informasi (KAMI)	76
17. Pengukuran Indeks KAMI	80
18. Opensource	83
19. Kejahatan Komputer Dari Pandangan Keislaman	84
BAB III METODE PENELITIAN	90
A. Studi Literatur.....	90
B. Pre-Assessment <i>Indeks KAMI</i> jaringan IBISA Purworejo	91
C. Implementasi Infrastruktur <i>ManageEngine OpMananager</i> jaringan IBISA INDONESIA.....	92
D. Monitoring.....	92
E. Post- Assessment <i>Indeks KAMI</i> jaringan IBISA Purworejo.....	92
F. Analisis Data	93
BAB IV ANALISIS DAN PEMBAHASAN	94
A. <i>Indeks Kami</i>	94
1. Mengkaji Hasil <i>Indeks Kami</i>	99

2. Tata kelola Keamanan Informasi	102
3. Pengelolaan Risiko Keamanan Informasi.....	105
4. Kerangka Kerja Pengelolaan Keamanan Informasi.....	108
6. Teknologi dan Keamanan Informasi.....	114
7. Rekomendasi.....	119
B. Implementasi ManageEngine OpManager	124
C. Monitor Trafik Pada Jaringan.....	126
D. Post-Assessment Indeks KAMI Jaringan IBISA Purworejo.....	133
E. Analisis Data	135
BAB V PENUTUP.....	144
A. Kesimpulan	144
B. Saran.....	145
DAFTAR PUSTAKA	146
LAMPIRAN.....	150
DAFTAR RIWAYAT HIDUP.....	197

DAFTAR GAMBAR

Gambar 2. 1 Arsitektur LAN.....	43
Gambar 2. 2 Arsitektur MAN.....	44
Gambar 2. 3 Arsitektur WAN	45
Gambar 2. 4 Logo mikrotik.....	48
Gambar 2. 5 CIA Triads (Y. Sattarova Feruza T. -H.Kim, 2007).....	50
Gambar 2. 6 arsitektur SNORT IDS.....	66
Gambar 2. 7 Arsitektur OpManager.....	75
Gambar 2. 8 Grafik Indeks KAMI	77
Gambar 2. 9 Matriks Kategori SE dan Status kepuasan Indeks KAMI 4.1	81
Gambar 2. 10 Nilai Kategori Sistem Elektronik	82
Gambar 2. 11 Tingkat kematangan dan kesiapan ISO27001	83
Gambar 3. 1 Metodologi Penelitian.....	90
Gambar 4. 1 Tingkat Kematangan Indeks KAMI	97
Gambar 4. 2 Hubungan Indeks Kami dengan ISO 27001	99
Gambar 4. 3 Dashboard Pre-Assessment Indeks KAMI IBISA Purworejo	101
Gambar 4. 4 Diagram Trafik jaringan IBISA.....	128
Gambar 4. 5 Dashboard Post-Assessment Indeks KAMI jaringan IBISA.....	134
Gambar 4. 6 Nilai Indeks KAMI Pre dan Post-Assessment Jaringan IBISA.....	135

DAFTAR TABEL

Tabel 2. 1 Perbandingan Tinjauan Pustaka	29
Tabel 2. 2 Informasi di dalam aplikasi Ntop	62
Tabel 4. 1 Skor kematangan area tata kelola keamanan informasi(i)	102
Tabel 4. 2 Skor Kematangan Area Tata Kelola Keamanan Informasi(ii)	104
Tabel 4. 3 Skor kematangan area Pengelolaan Risiko Keamanan Informasi(i).....	105
Tabel 4. 4 Skor Kematangan Area Pengelolaan Risiko Keamanan Informasi (ii).....	107
Tabel 4. 5 Skor kematangan area Kerangka kerja Keamanan Informasi (i)	108
Tabel 4. 6 Skor Kematangan Area Kerangka Kerja Keamanan Informasi (ii).....	110
Tabel 4. 7 Skor kematangan area Pengelolaan Aset Informasi (i)	112
Tabel 4. 8 Skor Kematangan Area Pengelolaan Aset Informasi (ii) .	112
Tabel 4. 9 Skor area keraangka Teknologi dan Keamanan Informasi (i)	114
Tabel 4. 10 Skor Kematangan Area Kerangka Teknologi dan Keamanan Informasi (ii).....	115
Tabel 4. 11 Hasil Tingkat Kematangan	117
Tabel 4. 12 Rekomendasi Pengelolaan Risiko Keamanan Informasi	119
Tabel 4. 13 Rekomendasi Tata Kelola Keamanan Informasi.....	120
Tabel 4. 14 Rekomendasi Kerangka Kerja Pengelolaan Keamanan Informasi.....	121
Tabel 4. 15 Rekomendasi Pengelolaan Aset Informasi.....	122

Tabel 4. 16 Rekomendasi Teknologi dan Keamanan Informasi	123
Tabel 4. 17 Trafik jaringan IBISA (i).....	127
Tabel 4. 18 Trafik jaringan IBISA (ii).....	132
Tabel 4. 19 Pre-Aseesment Aspek “Tata Kelola Keamanan Informasi”	136
Tabel 4. 20 Post-Aseesment Aspek “Tata Kelola Keamanan Informasi”	137
Tabel 4. 21 Pre-Aseesment Aspek “Pengelolaan Aset Informasi” ...	138
Tabel 4. 22 Post-Aseesment Aspek “Pengelolaan Aset Informasi” .	139
Tabel 4. 23 Pre-Aseesment Aspek “Teknologi dan Keamanan Informasi”	140
Tabel 4. 24 Post-Aseesment Aspek “Teknologi dan Keamanan Informasi”	141



DAFTAR SINGKATAN

KAMI	: <i>Keamanan Informasi</i>
SIEM	: <i>Security Information and Event Management</i>
IDS	: <i>Intrusion Detection System</i>
TCP	: <i>Transmission control protocol</i>
UDP	: <i>Use Datagram Protocol</i>
ICMP	: <i>Internet Control Message Protocol</i>



STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

BAB I PENDAHULUAN

A. Latar Belakang

Banyaknya pengguna layanan serta pengaruh internet maka akan semakin banyak pula informasi yang didapatkan dari internet. Di seluruh dunia terdapat sekitar 650 *terabyte* data dan 205 juta *email* di kirim melalui internet setiap menit nya. Perencanaan, desain dan implementasi topologi jaringan, dalam hal ini jaringan komputer nirkabel, tidak dapat diandalkan seperti itu. Perluasan jaringan komputer akan berdampak besar pada kualitas layanan koneksi internet dan kondisi pertukaran data yang ada. Kualitas dari layanan internet maupun koneksi pertukaran data setelah adanya perluasan jaringan maka tentu akan sangat penting untuk merubah performa dari jaringan komputer itu sendiri.

Sesuai dengan Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Standar Sistem Manajemen Keamanan Informasi, setiap instansi pemerintah wajib mematuhi SMKI dan memiliki nilai CIA (Confidentiality, Availability and Integrity) untuk aset informasi. Menurut penelitian yang dilakukan oleh tim Iccsindia, yang menjelaskan bahwa kerugian kejahatan dunia maya diperkirakan mencapai 6 triliun dan 60 juta catatan dikompromikan karena cloud tidak dikonfigurasi sesuai dengan keamanan siber. Pelanggaran keamanan terjadi di bisnis kecil, dengan total 43% serangan. 56% pelanggaran data membutuhkan waktu lebih dari sebulan untuk menemukan penangannya. Itu

kemudian dikuatkan oleh data tentang serangan ransomware paling umum yang ditemui pada tahun 2019, tetapi WannaCry terus memakan korban di seluruh dunia, dan laporan baru menunjukkan itu tetap menjadi infeksi ransomware nomor satu tahun lalu.

WannaCry ditangkap di lebih dari 23,5 persen perangkat yang akhirnya menjadi sasaran ransomware, dan email spam dan phishing tetap menjadi sumber infeksi paling umum tahun lalu, kata Precise Security. Tidak kurang dari 67% infeksi ransomware dikirim melalui email, dan kurangnya pelatihan keamanan siber serta kata sandi yang lemah dan manajemen akses adalah alasan berikutnya mengapa komputer akhirnya dienkrpsi setelah serangan. Hanya 16% serangan ransomware yang didukung oleh situs web jahat dan iklan online. "Jumlah serangan ransomware yang menargetkan lembaga pemerintah, organisasi di sektor kesehatan, energi, dan pendidikan terus meningkat.

Sementara beberapa ransomware sederhana dapat mengunci sistem dengan cara yang tidak sulit bagi orang yang berpengetahuan untuk membalikkannya, malware yang lebih canggih mengeksploitasi a teknik yang disebut crypto-virus ransomware. (Dewantara and Sugiantoro, 2021)

Karena semakin banyak cara mengakses data dan teknologi yang digunakan berkembang, tentu saja hal ini akan menyebabkan peningkatan ancaman keamanan terhadap jaringan. Hal ini tentunya sangat berbahaya terutama di bidang keamanan data dimana data guru bersifat sensitif. Oleh karena itu, perhatian khusus perlu diberikan pada bidang keamanan siber yang ditujukan untuk

mencegah pencurian data perusahaan. Dilihat dari pengertian dan jenis-jenis cybercrime, cybercrime merupakan bentuk kejahatan modern. Dan Oleh karena itu, kejahatan dunia maya dianalisis menurut hukum Islam (jinayat) Bisa dihukum dengan ta'zir. Ta'zîr artinya pencegahan menurut bahasanya (al-man'u). Adapun istilah ta'zîr adalah hukuman pendidikan (ta'dîb), artinya diramalkan dengan menakut-nakuti (tankîf). Adapun syar', ta'zîr dimaksudkan sebagai sanksi berdasarkan ketidaktaatan, karena secara tegas dikecualikan dari kejahatan yang terkandung dalam Al-Qur'an dan Hadis. Allah SWT melarang manusia untuk melanggar hak-hak orang lain, seperti ketidakpercayaan, penipuan dan pencurian, yang secara jelas ditunjukkan dalam ayat-ayat Al-Qur'an, yang melarang manusia melakukan kesalahan. Hal ini juga bertentangan dengan tujuan utama Nabi Rasulullah sebagai utusan Allah, yang memberikan teladan hidup akhlak yang baik kepada umat manusia. (H.Sofwan Jannah, n.d.2012)

Institut Teknologi Bisnis Dan Kesehatan Bhakti Putra Bangsa Indonesia (IBISA) adalah salah satu perguruan tinggi atau kampus yang berada di Purworejo Jawa Tengah. IBISA memiliki Pusat Pangkalan Data dan Informasi (PUSDATIN) Kampus IBISA memiliki juga memiliki layanan sistem informasi yaitu: Pendaftaran mahasiswa baru IBISA melalui sistem online, Layanan sistem informasi akademik untuk mahasiswa, dosen dan akademik, Data alumni dan Tracer Studi, Sistem layanan ujian online, Elearning terintegrasi dengan sistem akademik, Sistem persuratan terintegrasi dan Sistem Pengelolaan kepegawaian terintegrasi.

Dengan kebutuhan untuk lembaga pemerintah untuk dapat menerapkan standar manajemen keamanan informasi sesuai dengan SMKI dan kebutuhan untuk melacak ke masyarakat adalah pilihan absolut sehingga petugas perlindungan dapat dengan jelas melihat apa yang terjadi dengan jaringannya. Pertanyaannya adalah apakah penggunaan Ossim dapat mendeteksi semua serangan pada jaringan dan secara efektif mengamankan jaringan dari serangan yang ada. Terutama dalam hal pemantauan server dan jaringan, tentu saja, administrator tidak dapat bekerja 24 jam di depan komputernya sehingga selalu tahu jika ada gangguan pada server dan jaringan. (Angga Juansyah, Bagus Pratama, 2018), oleh karena itu fasilitas pendukung diperlukan oleh sistem perdagangan administrator dapat memonitor server dan jaringan meskipun mereka tidak berada di depan komputer secara langsung, sehingga sistem pelacakan diperlukan yang dapat memonitor server mereka dan Jaringan selama 24 jam dan dapatkan pemberitahuan langsung ke admin. Sebelum standar keamanan informasi diterapkan, evaluasi perangkat keamanan informasi di jaringan IBISA Indonesia diperlukan untuk mendapatkan gambaran tentang kondisi kesiapan dan kematangan manajemen keamanan informasi. Berdasarkan hal ini, penelitian ini akan mengukur tingkat kematangan manajemen keamanan informasi pada jaringan IBISA Indonesia menggunakan versi yang disiapkan oleh komunikasi Indonesia pada tahun 2019, yaitu *Indeks* kami. *Indeks* kami dibuat dengan ISO 27001: 2018 Referensi yang berisi keamanan informasi ISO 27001 adalah bentuk kerangka kerja standar internasional yang berisi standar di

wilayah keamanan informasi, ruang lingkup penggunaan teknologi dan manajemen aset yang membantu organisasi memastikan bahwa keamanan informasi telah berjalan dengan efektif.

Berdasarkan latar belakang diatas, penulis membuat penelitian yang berjudul “Optimasi Keamanan Informasi Dengan Security Information and Event Managemen (SIEM) ManageEngine OpManager studi Kasus: PUSDATIN IBISA Purworejo”.

B. Rumusan Masalah

Dari latar belakang dan permasalahan yang telah disampaikan, permasalahan yang menjadi fokus pada penelitian ini adalah:

1. Bagaimana menganalisis Sistem Informasi Akademik IBISA INDONESIA sehingga dapat mencukupi kebutuhan informasi dari pengguna dalam melakukan pertukaran data dengan melakukan penelitian dengan menggunakan metode *ManageEngine OpMananager* dan aplikasinya pada *Indeks Keamanan Informasi (KAMI)*
2. Bagaimana memonitoring *server* pada Sistem Informasi Akademik IBISA INDONESIA dalam melakukan proses perjalanan data di dalam sebuah jaringan komputer yang memiliki jumlah *client* yang banyak dan aktifitas jaringan komputer dalam skala besar

C. Batasan Masalah

Agar permasalahan pada penelitian ini tidak meluas, maka perlu adanya batasan terhadap masalah diantaranya sebagai berikut:

1. Daerah atau lokasi hanya pada Sistem Informasi Akademik kampus IBISA INDONESIA.
2. Menggunakan *software* yaitu *ManageEngine OpManager* pada server yang dirancang.
3. Pengujian sistem dilakukan dengan simulasi di IBISA INDONESIA.
4. Menggunakan kuesioner untuk mengetahui celah sistem yang berjalan pada *Indeks* Keamanan Informasi (KAMI).

D. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1. Menganalisa dan menggambarkan untuk mendapatkan hasil yang akurat terhadap keamanan informasi pada sistem informasi akademik serta meningkatkan kualitas keamanan informasi.
2. Memantau dan agar dapat mengetahui lebih detail akan permasalahan yang ada pada jaringan IBISA INDONESIA sehingga dapat diketahui solusi yang dapat digunakan untuk mengatasi sehingga dapat memaksimalkan infrastruktur jaringan komputer yang ada agar lebih optimal sebagaimana fungsinya sebagaimana institusi pendidikan.
3. Mengetahui hasil dari penerapan *Security Information And Event Management* (SIEM) Dan Implikasinya Pada *Indeks* Keamanan Informasi (KAMI) pada jaringan IBISA INDONESIA dengan Menciptakan sistem pendeteksi atau sensor terhadap area jaringan menggunakan aplikasi berbasis open source, yaitu *ManageEngine OpManager* Oleh karena

itu, laporan diberikan kepada administrator sistem tentang percobaan serangan pada sistem melalui log yang dihasilkan oleh aplikasi sebagai bukti digital dari setiap percobaan serangan atau penyusupan ke dalam area server.

E. Manfaat Penelitian

Adapun penelitian ini diharapkan dapat memberikan manfaat, diantaranya yaitu:

1. Bagi pengguna, akan mendapatkan pengetahuan dalam penggunaan jaringan di dalam suatu instansi untuk memperoleh informasi yang dibutuhkan.
2. Bagi penulis, dapat digunakan sebagai acuan untuk mendokumentasikan serta memberikan laporan secara terperinci kepada administrator sistem terkait dengan kondisi keamanan dari lalu lintas jaringan, sehingga dapat dilakukan tindakan pencegahan terhadap upaya penyerangan guna menjaga stabilitas dari layanan yang tentunya telah sesuai dengan kondisi jaringan komputer yang ada di IBISA INDONESIA.
3. Sebagai salah satu solusi pada *Network Administrator* yang lebih sesuai dengan kebutuhan yang dapat berjalan sebagaimana dengan fungsinya sehingga dapat menjadikan jaringan menjadi lebih optimal dengan perannya sebagai Institusi Pendidikan.
4. Manfaat yang ini diperoleh dari penelitian ini adalah dapat memperkecil kemungkinan terjadinya kegagalan pada sistem server sehingga akses lalu lintas jaringan yang ada dapat

berjalan dengan baik sebagaimana mestinya dan dengan biaya seminimal mungkin dengan hasil semaksimal mungkin.

F. Keaslian Penelitian

Penelitian yang terkait dengan monitoring jaringan sudah pernah dilakukan seperti implementasi Open Source Security Information Management (OSSIM). Akan tetapi penelitian tentang “Optimasi Keamanan Informasi dengan Security Information and Event Management (SIEM) *ManageEngine OpManager* (Studi Kasus: IBISA purworejo)” belum pernah dilakukan sebelumnya.

G. Sistematika Penulisan

Sistematika penulisan pada penelitian ini terdiri dari lima bab, dengan sistematika berikut:

- Bab 1 Pendahuluan
Membahas tentang latarbelakang penggunaan *ManageEngine OpMananager* dalam suatu organisasi. Pada bab ini juga membahas tentang Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Metodologi Penelitian dan Sistematika Penulisan laporan pada penelitian yang dilakukan.
- Bab 2 Tinjauan Pustaka
Membahas tentang teori dasar yang digunakan dalam penelitian, terkait *ManageEngine OpMananager*, *Indeks KAMI*. Pada bab ini juga membahas mengenai tinjauan pustaka terkait dengan penelitian yang pernah dilakukan sebelumnya.

- Bab 3 Metode Penelitian

Membahas tentang langkah-langkah penelitian, analisis kebutuhan dan perancangan sistem, membahas analisis terhadap kebutuhan sistem yang dibangun, proses kerja dan perancangan sistem yang meliputi: Topologi, Infrastruktur, pilihan *Software* dll.

- Bab 4 Analisis dan Pembahasan

Membahas hasil penelitian yang berupa eksekusi model dan pengujian parameter.

- Bab 5 Penutup

Membahas tentang kesimpulan yang berupa rangkuman dari hasil dan pembahasan pada bab -bab sebelumnya serta saran yang perlu diperhatikan berdasarkan batasan yang ditemukan dan asumsi yang ada selama dilakukannya penelitian untuk perbaikan dan pengembangan selanjutnya.

BAB V

PENUTUP

A. Kesimpulan

1. Tingkat Kematangan dan integritas keamanan informasi jaringan IBISA Purworejo masih rendah. alasan rendah Integritas dan tingkat kematangan keamanan informasi ini adalah Jaringan IBISA Purworejo belum sepenuhnya melaksanakan Persyaratan keamanan informasi atau masih dalam perencanaan. Rendahnya tingkat kelengkapan ditunjukkan pada bar chart yang Menampilkan warna merah dengan total nilai 174, warna kuning dengan total nilai 312 dan warna Hijau Muda menunjukkan total nilai 535. Hal ini mengartikan bahwa keamanan informasi pada jaringan IBISA Purworejo tidak layak dan perlu banyak perbaikan. Sedangkan tingkat kematangan untuk setiap area keamanan informasi berada pada level I sampai dengan II. Kemudian sebagai kebijakan standar ISO/IEC 27001:2018, Tanggal kedaluwarsa yang diharapkan untuk ambang batas minimum Kesiapan sertifikasi adalah berada pada Level atau tingkat kematangan III+.
2. Terkait dengan Indeks Keamanan Informasi (KAMI) pada penggunaan teknologi *ManageEngine OpMananager* terbukti dapat meningkatkan nilai dari Indeks Keamanan Informasi (KAMI) pada jaringan IBISA Purworejo pada berbagai aspek. Peningkatan nilai-nilai pada berbagai aspek tidak lepas dari peranan penggunaan teknologi *ManageEngine OpMananager*

dalam menganalisa yang menjadi kelemahan dan perubahan konfigurasi aset informasi pada jaringan IBISA Purworejo. *ManageEngine OpMananager* juga dapat melakukan monitoring serta melakukan proses Analisa terhadap aset dan jaringan IBISA Purworejo secara sistematis.

B. Saran

Rekomendasi ataupun untuk penelitian selanjutnya adalah Membangun kesadaran di antara staf PUSDATIN IBISA Purworejo berkaitan dengan keamanan informasi. staf terlebih dahulu menyadari pentingnya perlindungan keamanan informasi dari Semua aspek yang terkait dengan keamanan informasi dalam Mendukung kinerja jaringan. indeks KAMI paling tidak digunakan satu tahun sekali sebagai alat Tinjauan terhadap kesiapan keamanan informasi serta Mengevaluasi keberhasilan perbaikan yang telah dilaksanakan dengan mencapai tingkat kelengkapan atau kematangan tertentu.

DAFTAR PUSTAKA

- Achmad, B., Nur, I. W. and Siti, K. (2019) ‘*Development of Linux Ubuntu Open Source Distribution Based Open Source Distribution System to Minimize Students ‘Software Study’*’, 287(Icesre 2018).
- Adi Reynaldo, Sengkey Rizal, P. (2020) ‘Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI’, *Jurnal Teknik ...*, pp. 189–198. Available at: <https://ejournal.unsrat.ac.id/index.php/informatika/article/view/31597>.
- Angga Juansyah, Bagus Pratama, I. D. (2018) ‘Analisis dan implementasi open source security information managment (ossim) pada keamanan jaringan komputer pt. satria antaran prima palembang’. Available at: <http://library.palcomtech.com/pdf/5621.pdf>.
- Arfanudin, C. *et al.* (2019) ‘Analisis Serangan Router Dengan Security Information and Event Management (Siem) Dan Implikasinya Pada Indeks Analysis of Router Attack With Security Information and Event Management and Implications (Siem) in Information Security’, 2(1), pp. 1–7.
- Ari Prsyogi, Maylane Boni, S. S. (2019) ‘No’, 45(45), pp. 95–98.
- Darwis, D. and Solehah, N. Y. (2021) ‘PENERAPAN FRAMEWORK COBIT 5 UNTUK AUDIT TATA KELOLA KEAMANAN INFORMASI PADA KANTOR WILAYAH KEMENTERIAN’, 1(2), pp. 38–45.
- Dewantara, R. (no date) *Oleh : Nama NIM : Rizki Dewantara.*
- Dewantara, R. and Sugiantoro, B. (2021) ‘Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta)’, *Jurnal Teknologi Informasi dan Ilmu Komputer*, 8(6), p. 1137. doi: 10.25126/jtiik.2021863123.

- H.Sofwan Jannah, M. . naufa. (no date) ‘PENEGAKAN HUKUM CYBER CRIME DITINJAU DARI Abstract ’, XII(1), pp. 69–84.
- Hermawan, W. (2019) ‘Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE)’, *Jurnal Telekomunikasi dan Komputer*, 9(2), p. 129. doi: 10.22441/incomtech.v9i2.6474.
- Husna, M. A. and Rosyani, P. (2021) ‘Implementasi Sistem Monitoring Jaringan dan Server Menggunakan Zabbix yang Terintegrasi dengan Grafana dan Telegram’, *Jurnal Riset Komputer*, 8(6), pp. 2407–389. doi: 10.30865/jurikom.v8i6.3631.
- Kamal, M. R. and Setiawan, M. A. (2021) ‘Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII’, *Automata*, (4).
- Kornelia, A. and Irawan, D. (2021) ‘Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1’, *Jurnal Pengembangan Sistem Informasi dan Informatika*, 2(2), pp. 78–86. doi: 10.47747/jpsii.v2i2.548.
- Kristanto, T. *et al.* (2019) ‘Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ’, *JISA(Jurnal Informatika dan Sains)*, 2(2), pp. 30–33. doi: 10.31326/jisa.v2i2.497.
- 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. Available at: <http://speed.web.id/jurnal/index.php/speed/article/view/220>.
- Mahardika, F. (2017) ‘Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)’, 02(02), pp. 1–8.
- Miftah, Z. (2019) ‘Penerapan Sistem Monitoring Jaringan Dengan Protokol Snmp Pada Router Mikrotik Dan Aplikasi Dude Studi Kasus Stikom Cki’, *Faktor Exacta*, 12(1), p. 58. doi:

10.30998/faktorexacta.v12i1.3481.

- Nofry Arman, Widhy Hayuhardhika Nugraha Putra, A. R. (2019) '3. Tampilan Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI).pdf'.
- Pamungkas, W. C. and Saputra, F. T. (2020) 'Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013', *Jurnal Sistem Komputer dan Informatika (JSON)*, 1(2), p. 101. doi: 10.30865/json.v1i2.1924.
- Prasetyowati, D. D. *et al.* (2019) 'Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang', *JOINS (Journal of Information System)*, 4(1), pp. 65–75. doi: 10.33633/joins.v4i1.2429.
- Rahmat Hidayat, Mohammad Suyanto, A. S. (2018) 'P Rogram S Tudi D Oktor', *Pemodelan Arsitektur Sistem Informasi Perizinan Menggunakan Kerangka Kerja Togaf Adm*, 4(1), p. 113.
- Rakhmat Dwi Jayanto (2019) 'Rancang Bangun Sistem Monitoring Jaringan Menggunakan Mikrotik Router OS', *JATI (Jurnal Mahasiswa Teknik Informatika)*, 3(4), pp. 391–395.
- Riani, R. *et al.* (2018) 'Implementasi Monitoring Lalu Lintas Jaringan Dengan Ntop pada Jaringan Dual Stack Implementation of Network Traffic Monitoring With Ntop on DualStack Networks', *Techno.COM*, 17(4), pp. 424–432.
- Riswaya, A. R. *et al.* (2020) 'Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks Kami Untuk Persiapan Standar Sni Iso/Iec 27001 (Studi Kasus: Stmik Mardira Indonesia)', *Jurnal Computech & Bisnis*, 14(1), pp. 10–18.
- Sutarti, Adi Putranto Pancaro, F. I. S. (2018) 'Implementasi Ids (Intrusion Detection System)', *Jurnal PROSISKO*, 5(1).

- WIJATMOKO, T. E. (2020) 'Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy', *Cyber Security dan Forensik Digital*, 3(1), pp. 1–6. doi: 10.14421/csecurity.2020.3.1.1951.
- Wijaya, Y. D. (2021) 'Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013', *Jurnal Sistem Informasi dan Informatika (Simika)*, 4(2), pp. 115–130. doi: 10.47080/simika.v4i2.1178.
- Yasin, A. and Mohidin, I. (2018) 'Monitoring DDOS Pada Openflow Switch Dengan Alienvault Ossim', *Jurnal Teknologi Informasi Indonesia (JTII)*, 3(2), p. 23. doi: 10.30869/jtii.v3i2.260.
- Yauma Dzikri Imany, Widhy Hayuhardika Nugraha Putra, admaja D. H. (2019) 'Tampilan Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia).pdf'.
- Yunella, Dwi Herlambang, Nugraha Putra, M. (2019) 'Tampilan Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI.pdf'.