OPTIMASI PADA SECURITY INFORMATION EVENT MANAGEMENT MENGGUNAKAN ARCSIGHT DAN SECURITY OPERATION CENTRE FRAMEWORK (STUDI KASUS : PADA SUATU BANK MULTINASIONAL)

TESIS

Willy Pratama
1511600064

PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2017

OPTIMASI PADA SECURITY INFORMATION EVENT MANAGEMENT MENGGUNAKAN ARCSIGHT DAN SECURITY OPERATION CENTRE FRAMEWORK (STUDI KASUS : PADA SUATU BANK MULTINASIONAL)

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)

Willy Pratama
1511600064

PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2017

LEMBAR PERNYATAAN

PROGRAM STUDI MAGISTER ILMU KOMPUTER

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini

Nama Mahasiswa : Willy Pratama
Nomor Induk Mahasiswa : 19116000 64
Konsentrasi : Teknologi Sistem Informasi
Program Studi : Magister Ilmu Komputer
Fakultas / Program : Pascasarjana

Menyatakan bahwa Tesis dengan judul :

Optimasi Pada Security Information Event Management menggunakan Arc Sight dan Security Operation Centre Framework (Studi Kasus : pada Suatu Bank Multinasional)

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. saya mengizinkan Universitas Budi Luhur untuk mengelola sesuai dengan hukum dan etika yang berlaku

Pernyataan ini saya buat dengan penuh rasa tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 1 Agustus 2017

Willy Pratama

ii

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa	:	Willy Pratama
Nomor Induk Mahasiswa	:	1511600064
Konsentrasi	:	Teknologi Sistem Informasi
Program Studi	:	Magister Ilmu Komputer
Judul Tesis	:	Optimasi Pada Security Information Event Management menggunakan ArcSight dan Security Operation Centre Framework (Studi Kasus : pada Suatu Bank Multinasional)

Jakarta, 01 Agustus 2017

Tim Penguji — Tanda Tangan

Ketua,
(Dr. M. Syafrullah, M.Kom., M.Sc.) .....

Anggota,
(Ir. Wendi Usino, MM., M.Sc., Ph.D) .....

Pembimbing Utama,
(Dr. Ir. Nazori AZ, M.T.) .....

Ketua Program Studi
Magister Ilmu Komputer

(Dr. M. Syafrullah, M.Kom., M.Sc.)

ABSTRAK

Semakin banyak peralatan keamanan jaringan yang diimplementasikan, maka semakin banyak pula peralatan yang perlu dikelola dan di monitor. Semakin banyak peralatan yang dipasang, maka semakin banyak *log-log* yang dihasilkan. *Security Information Event Management* mampu menyediakan informasi yang terkait dengan keamanan jaringan secara terpusat. Dengan berkembangnya *financial technology* di Indonesia tentu diperlukan suatu regulasi dan sistem keamanan teknologi informasi. Pada penelitian ini penulis melakukan optimasi berdasarkan rule, filter dan atribut yang dibutuhkan oleh SIEM sehingga informasi yang dihasilkan oleh dasbor hanya informasi yang dibutuhkan saja. Optimasi yang dilakukan yaitu menyaring dan mengkonfigurasi mesin SIEM sesuai dengan data keluaran yang bersifat false positive. SOC Framework berguna sebagai acuan dasar dalam membentuk Incident Response Team yang memonitor segala aktifivitas selama 24 jam penuh, dengan perpaduan SIEM dan SOC framework ini dapat dijadikan upaya untuk menahan dan memberantas *cyber-security* di internal dan eksternal jaringan keamanan anda. Hasil optimasi yang telah dilakukan yaitu berdasarkan dasbor utama dengan rentang waktu 10, 120 dan 1440 menit dengan efisiensi yang dihasilkan 1.908 %, 6.567 % dan 19.874 %, dari pengujian tersebut dapat dibuktikan optimasi yang dilakukan sangat berpengaruh terhadap kinerja SIEM.

Kata Kunci: *SIEM, Cyber-security, security operation centre framework, financial technology, Incident Response Team,*

ABSTRACT

The more network security equipment is implemented, the more equipment that needs to be managed and monitored. The more equipment installed, the more logs are generated. Security Information Event Management is able to provide information related to network security centrally. With the development of financial technology in Indonesia would require a regulation and information technology security system. In this study the authors do the optimization based on rules, filters and attributes required by SIEM so that the information generated by the dashboard only the required information only. Optimization is done that filter and configure the SIEM engine in accordance with the output data that is false positive. The SOC Framework is useful as a basic reference in establishing an Incident Response Team that monitors all 24-hour active activities, with the SIEM and SOC framework combined to cope and combat cyber-security in your internal and external security networks. The result of optimization that has been done is based on the main dash with 10, 120 and 1440 minutes with the efficiency of 1.908%, 6.567% and 19.874%, from the test can be proved that the optimization is very influential on SIEM performance.

Keywords : SIEM, Cyber-security, security operation centre, framework, financial technology. Incident response team

KATA PENGANTAR

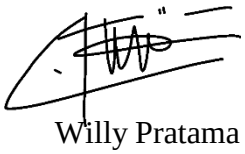
Puji dan syukur senantiasa kepada Tuhan Yang Maha Esa yang telah memberikan kekuatan dan hikmat sehingga penulis dapat menyelesaikan tesis yang berjudul "**Optimasi Pada Security Information Event Management menggunakan ArcSight dan Security Operation Centre Framework (Studi Kasus : Pada suatu Bank Multinasional)**".

Dalam kesempatan ini penulis ingin menyampaikan rasa terima kasih kepada semua pihak yang telah memberikan bantuan atas penyelesaian penulisan tesis ini, diantaranya:

1. Keluarga besar yang senantiasa memberikan kasih sayang, nasihat, dorongan serta do'a yang tak pernah berhenti mengalir.
2. Bapak Dr. Ir. Nazori Az, M.T selaku Dosen Pembimbing Utama program Pascasarjana Universitas Budi Luhur yang telah banyak memberikan saran dan masukan dalam penyusunan tesis ini.
3. Bapak Prof. Dr. Sc. Agr. Ir. Didik Sulistyanto selaku Rektor Universitas Budi Luhur.
4. Bapak Dr. Suhartono, M.A, MBA selaku Direktur Program Pascasarjana Universitas Budi Luhur.
5. Bapak Dr. M. Syafrullah, M.Kom, M.Sc selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
6. Seluruh dosen dan staff Universitas Budi Luhur yang telah memberikan bantuan serta semua pihak yang memberikan waktu dan masukan dalam pembuatan tesis ini.
7. Seluruh kawan-kawan satu angkatan 2015, terkhusus kelas BI jurusan Teknologi Sistem Informasi.
8. Nadia Noviani, S.Kom. yang telah memberikan banyak dukungan dalam penyelesaian tesis ini.

Penulis menyadari penulisan tesis ini masih jauh dari sempurna. Untuk itu penulis mengharapkan kritik dan saran yang membangun demi tercapainya penulisan yang lebih baik.

Jakarta, 1 Agustus 2017



Willy Pratama

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

A., F.A. & Y., F.S. 2009. Methodology for Penetration Testing.

David Miller, Harris, Harper, S., AllenVanDyke, Blask, S. & Chris 2011. *Security Information and Event Management (SIEM) Implementation*. The McGraw - Hill Companies.

Guritno, S., Sudaryono & Rahardja, U. 2011. *Theory and Application of IT Research-Metodologi dan Penelitian Teknologi Informasi*. Yogyakarta: Andi.

Hewlett-Packard 2013. *Concepts for ArcSight Express 4.0 with CORR-Engine*. Hewlett-Packard Development Company,.

ISO ORG 2013. *International Organization for Standardization*. Tersedia di https://www.iso.org/isoiec-27001-information-security.html.

Keuangan, O.J. 2016. Regulasi Fintech di Indonesia.

Kotenko, I., Polubelova, O. & Saenko, I. 2012. The ontological approach for SIEM data repository implementation. *Proceedings - 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCom 2012*. hal.761–766.

Montesino, R., Fenz, S. & Baluja, W. 2012. SIEM-based framework for security controls automation. *Information Management & Computer Security*, 20(4): 248–263. Tersedia di http://dx.doi.org/10.1108/09685221211267639%5Cnhttp://dx.doi.org/10.1108/IMCS-07-2013-0053%5Cnhttp://dx.doi.org/10.1108/IMCS-05-2013-0041%5Cnhttp://.

Riduwan 2004. *Metode & Teknik Menyusun Tesis*. Jakarta: Alfabeta.

Rihal, M. 2010. *Implementasi dan Analisa Security Information Management Menggunakan OSSIM pada Sebuah Perusahaan*. Universitas Indonesia.

Schumpeter, J.A. 1934. *The Theory of Economic Development: An Inquiry Into Profits, Capital, Credit, Interest, and the Business Cycle*.