



**ANALISIS *LOG* SISTEM PADA *SECURITY INFORMATION AND EVENT
MANAGEMENT* UNTUK MENDETEKSI DATA *EXFILTRATION***

SKRIPSI

Tiara Sakinah

1810511031

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2022

PERNYATAAN ORISINALITAS

Skripsi ini merupakan hasil karya saya sendiri, dan semua kutipan dan sumber yang dirujuk telah saya nyatakan dengan benar.

Nama : Tiara Sakinah
NIM : 1810511031
Tanggal : 04 Juni 2022

Jika pada kemudian hari ditemukan ketidak sesuaian maka saya siap untuk diproses sesuai dengan peraturan yang berlaku

Jakarta, 04 Juni 2022

Yang Menyatakan,



(Tiara Sakinah)

**PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademika Universitas Pembangunan Nasional “Veteran”
Jakarta, saya yang bertanda tangan di bawah ini :

Nama : Tiara Sakinah
NIM : 1810511031
Fakultas : Ilmu Komputer
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

**Analisis Log Sistem Pada Security Information And Event Management
Untuk Mendeteksi Data Exfiltration**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 04 Juni 2022

Yang Menyatakan,



(Tiara Sakinah)

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

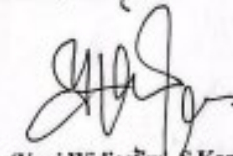
Nama : Tiara Sakinah
NIM : 1810511031
Program Studi : SI – Informatika
Judul : Analisis Log Sistem pada Security Information and Event Management untuk Mendeteksi Data Exfiltration

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi SI Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



(Bayu Hananto, S.Kom, M.Kom.)

Penguji I



(Yuni Widiastuti, S.Kom., Msi.)

Penguji II



(Henki Bayu Seta, S.Kom, MTL)

Pembimbing I



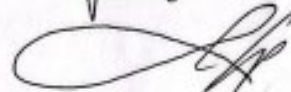
(I Wawan Widi P, S.Kom., MTL)

Pembimbing II



(Dr. Ermatita, M. Kom.)

Dekan Fakultas Ilmu Komputer



(Desta Sandya Prasvita, S. Komp., M.Kom.)

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Pengesahan : 1 Juli 2022



LEMBAR PERSETUJUAN

Dengan ini menyatakan bahwa proposal berikut:

Nama : Tiara Sakinah

NIM : 1810511031

Program Studi : Informatika

Judul : Analisis Log Sistem Pada Security Information And
Event Management Untuk Mendeteksi Data Exfiltration

Sebagai bagian persyaratan yang diperlukan untuk mengikuti ujian Sidang Skripsi pada Program Studi Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

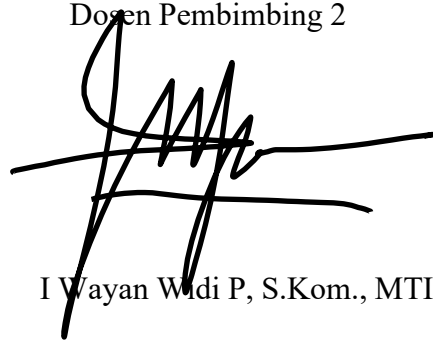
Menyetujui,

Dosen Pembimbing 1



Henki Bayu Seta, S.Kom, MTI

Dosen Pembimbing 2



I Wayan Widi P, S.Kom., MTI

Mengetahui, Ketua Program Studi



Desta Sandya Prasvita, S.
Komp., M.Kom.

Ditetapkan : Jakarta

Tanggal Persetujuan : 06 Juni 2022

ANALISIS LOG SISTEM PADA *SECURITY INFORMATION AND EVENT MANAGEMENT* UNTUK MENDETEKSI DATA *EXFILTRATION*

Tiara Sakinah

1810511031

Abstrak

Teknologi sangat erat kaitannya dengan data. Keberadaan teknologi adalah untuk menyampaikan kumpulan informasi dengan mudah dan efisien. Setiap individu maupun organisasi bertukar informasi dengan tujuan tertentu, dan banyak dari informasi tersebut yang memiliki tingkat keamanan yang tinggi. Pentingnya pengawasan pada setiap informasi merupakan aturan yang tidak bisa dilewatkan oleh setiap individu maupun organisasi. Kurangnya *awareness* pada keamanan data memancing kejahatan dengan mencuri data tersebut atau biasa disebut *data exfiltration*. Untuk mengatasi hal tersebut diatas, penulis menggunakan *Security Information and Event Management* atau disingkat SIEM. SIEM merupakan metode untuk mengumpulkan, menganalisa, memberi *alert* memberi laporan, serta melakukan automatisasi respon pada sebuah insiden. Penelitian ini diharapkan dapat menjabarkan hasil pengujian dan analisis serta memberikan rekomendasi solusi yang dapat dilakukan untuk mengatasi *data exfiltration* pada SIEM.

Kata kunci: *Sistem log, Security Information and Event Management, Data exfiltration*

**ANALISIS LOG SISTEM PADA SECURITY INFORMATION AND EVENT
MANAGEMENT UNTUK MENDETEKSI DATA EXFILTRATION**

Tiara Sakinah

1810511031

Abstract

Technology is closely related to data. The existence of technology is to convey a collection of information easily and efficiently. Each individual or organization exchanges information for a specific purpose, and much of that information has a high level of security. The importance of monitoring every piece of information is a rule that can not be missed by every individual or organization. Lack of *awareness* on data security provokes crime by stealing such data or commonly called *xfiltration data*. To overcome the above, the author uses *Security Information and Event Management* or abbreviated *siem*. SIEM is a method of collecting, analyzing, alerting ports, and automating responses to an incident. This research is expected to expand the results of testing and analysis and provide recommendations for solutions that can be done to overcome *exfiltration data* in SIEM.

Kata kunci: *Sistem log, Security Information and Event Management, Data exfiltration*

KATA PENGANTAR

Puji syukur Penulis panjatkan atas kehadiran Tuhan yang Maha Esa karena berkatnya Penulis dapat menyelesaikan pengerjaan Skripsi dengan judul “Analisis Log Sistem Pada Security Information And Event Management Untuk Mendeteksi Data Exfiltration” ini. Dengan ini penulis menyadari bahwa banyak pihak yang memberi dukungan dan bantuan selama pengerjaan Skripsi ini, oleh karena itu dengan penuh rasa hormat Penulis ingin mengucapkan terima kasih kepada:

1. Allah SWT, yang sudah memberikan kesehatan, kekuatan, dan kemudahan kepada penulis dalam menyelesaikan skripsi ini.
2. Mama penulis dan seluruh keluarga besar penulis yang selalu memberikan dukungan, doa, serta semangat untuk menyelesaikan Skripsi.
3. Bapak Henki Bayu Seta, S.Kom, MTI. Selaku dosen pembimbing I yang selama ini telah membantu dan memberikan saran, semangat dan masukan yang sangat bermanfaat dalam pengerjaan Skripsi ini.
4. Bapak I Wayan Widi P.,S.Kom., MTI. Selaku dosen pembimbing II yang selama ini telah membantu dan memberikan saran, semangat dan masukan yang sangat bermanfaat dalam pengerjaan Skripsi ini.
5. Ibu Dr. Ermatita, M.Kom. Selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
6. Bapak Bambang Tri Wahyono, S.Kom, M.Si. Selaku dosen pembimbing akademik.
7. Bapak/Ibu Dekan serta jajarannya dan seluruh dosen Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah memberikan ilmu-ilmu yang berguna dan dapat digunakan di masa yang akan datang kepada Penulis.
8. Seluruh rekan rekan penulis mengucapkan banyak terima kasih atas dukungan yang telah diberikan kepada penulis yang tidak dapat disebutkan satu per satu.
9. Rekan – rekan kerja tim Business Solution yang memberi Penulis semangat serta dukungan baik moril maupun materi.

Jakarta, 03 Juni 2022

Penulis

Daftar Isi

PERNYATAAN ORISINALITAS	i
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERSETUJUAN	iv
Abstrak	v
Abstract	vi
KATA PENGANTAR	vii
Daftar Isi	viii
Daftar Gambar.....	xi
Daftar Tabel	xiii
BAB I	1
PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Identifikasi Masalah	3
1.3. Rumusan Masalah	3
1.4. Batasan Masalah.....	4
1.5. Tujuan Penelitian.....	4
1.6. Manfaat Penelitian.....	4
1.7. Sistematika Penulisan.....	5
BAB II.....	7
LANDASAN TEORI DAN KAJIAN PUSTAKA	7
2.1. Data	7
2.2. Data Exfiltration.....	7
2.2.1. <i>Automated Exfiltration</i>	7
2.2.2. Data Transfer Size Limits	7
2.2.3. <i>Exfiltration Over Alternative Protocol</i>	8
2.2.4. <i>Over C2 Channel</i>	8
2.2.5. <i>Over Other Network Medium</i>	8
2.2.6. <i>Over Physical Medium</i>	8
2.2.7. <i>Over Web Service</i>	8
2.2.8. <i>Scheduled Transfer</i>	8
2.2.9. <i>Transfer Data to Cloud Account</i>	8

2.3.	Log.....	8
2.3.1.	Log keamanan perangkat lunak	9
2.3.2.	Log sistem operasi	9
2.4.	Syslog	9
2.5.	Security Information and Event Management.....	11
2.5.1.	Tahapan pada SIEM.....	11
2.5.2.	Arsitektur SIEM.....	11
2.6.	Log Management.....	12
2.7.	Security Information and Event Management dan Log Management....	13
2.8.	Wazuh.....	14
2.8.1.	Komponen Wazuh.....	16
2.8.2.	Arsitektur Wazuh	17
2.8.3.	Cara Kerja Wazuh.....	18
2.9.	Algoritma Advanced Encrypition Standard (AES).....	18
2.9.1.	Enkripsi	19
2.9.2.	Dekripsi.....	20
2.10.	Penelitian Terdahulu.....	21
BAB III		24
METODOLOGI PENELITIAN.....		24
3.1.	Kerangka Pikir.....	24
3.2.	Identifikasi Masalah	25
3.3.	Studi Literatur.....	25
3.4.	Perancangan Sistem.....	25
3.5.	Implementasi	28
3.6.	Hasil.....	28
3.7.	Alat Bantu Penelitian.....	29
3.7.1.	Perangkat keras	29
3.8.	Jadwal Penelitian.....	30
BAB IV		31
4.1.	Penyajian Data.....	31
4.1.1.	Perancangan Sistem	31
4.1.1.1.	Sistem Penyerangan.....	31
4.1.1.2.	Sistem Pemantauan.....	31
4.2.	Pengujian Data.....	36

4.3. Analisis Data	41
BAB V.....	47
5.1. KESIMPULAN	47
5.2. SARAN	48
Daftar Pustaka	49
RIWAYAT HIDUP.....	51
LAMPIRAN 1 Reporting Dashboard Format.....	52

Daftar Gambar

Gambar 1. 1 Hasil statistik Polisi Siber per Januari 2019 - November 2021.....	2
Gambar 2. 1 Syslog Windows.....	9
Gambar 2. 2 Arsitektur Syslog.....	10
Gambar 2. 3 Arsitektur SIEM	12
Gambar 2. 4 Tampilan dashboard Wazuh.....	16
Gambar 2. 5 Arsitektur Wazuh	17
Gambar 2. 6 Persamaan MixColumn.....	20
Gambar 2. 7 InvMixColumn.....	21
Gambar 3. 1 Kerangka Pikir	24
Gambar 3. 2 Rancangan Eksfiltrasi Data	26
Gambar 3. 3 Bagan Penyerangan.....	27
Gambar 3. 4 Rancangan Sistem Pemantauan.....	28
Gambar 4 1 Tampilan Wazuh.ova	31
Gambar 4 2 Tampilan dashboard Wazuh.....	32
Gambar 4 3 Wazuh Dashboard Custom oleh Penulis	32
Gambar 4 4 Perintah Membuat Dokumen Baru.....	32
Gambar 4 5 Security Alert	34
Gambar 4 6 Cara Membuat Agent	34
Gambar 4 7 Wazuh Agent Windows	35
Gambar 4 8 Wazuh Agent Linux	35
Gambar 4 9 Memetakan Direktori Pemantauan.....	36
Gambar 4 10 IP Penyerang	36
Gambar 4 11 IP Target Linux	37
Gambar 4 12 Folder Target.....	37
Gambar 4 13 Penyerang Berhasil Melakukan SSH	37
Gambar 4 14 auth.log Bukti SSH.....	38
Gambar 4 15 Proses Unduh dengan SCP.....	38
Gambar 4 16 Dokumen Terunduh	38
Gambar 4 17 Alert USB Terpasang.....	39
Gambar 4 18 Tampilan Konfigurasi pada agent.conf	39
Gambar 4 19 Pembuatan Dokumen dengan Format .exe untuk Mengirim Payload	39
Gambar 4 20 Lokasi SkripsiTiara.exe.....	40
Gambar 4 21 Aktifasi Virus	40
Gambar 4 22 Pengunduhan Dokumen	41
Gambar 4 23 Log SSH pada Wazuh	41
Gambar 4 24 Log SSH dengan SCP	43

Gambar 4 25 Log USB Terpasang.....	44
Gambar 4 26 Log USB Terlepas.....	44
Gambar 4 27 Log Eksekusi Virus.....	44
Gambar 4 28 File Integrity Monitoring.....	45
Gambar 4 29 Log pada ossec.log Wazuh Manager.....	46
Gambar 4 30 False Positive Logs.....	46

Daftar Tabel

<i>Tabel 2. 1 Perbedaan SIEM dan Log Management</i>	13
Tabel 2. 2 Perbandingan platform SIEM	14
Tabel 2. 3 Tabel S-box	19
Tabel 2. 4 Tabel Inversi S-box.....	21
Tabel 3. 1 Jadwal Penelitian.....	30
Tabel 4. 1 Hasil Percobaan	45