PEMANFAATAN TOOLS SIEM DENGAN AUTENTIKASI IoC UNTUK MONITORING PERANGKAT BERGERAK DI JARINGAN PERUSAHAAN

LAPORAN TUGAS AKHIR

HALAMAN J

MILLENITO NUR PRASETIYA
41518120063

UNIVERSITAS
MERCU BUANA

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2025

http://lib.mercubuana.ac.id
Menteng

PEMANFAATAN TOOLS SIEM DENGAN AUTENTIKASI IoC UNTUK MONITORING PERANGKAT BERGERAK DI JARINGAN PERUSAHAAN

LAPORAN TUGAS AKHIR

MILLENITO NUR PRASETIYA
41518120063

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2025

http://lib.mercubuana.ac.id
Menteng

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama	: Milllenito Nur Prastiya
NIM	: 41518120063
Program Studi	: Teknik Informatika
Judul Laporan Skripsi	: Pemanfaatan SIEM dengan Autentikasi IoC untuk Monitoring Perangkat Bergerak di Jaringan Perusahaan.

Menyatakan bahwa Laporan Skripsi ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan Skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Jakarta 22 Agustus 2023



Millenito Nu[illegible]

http://lib.mercubuana.ac.id
Menteng

UNIVERSITAS
MERCU BUANA
AKREDITASI UNGGUL

PERNYATAAN SIMILARITY CHECK
/SIMILARITY CHECK STATEMENT

Saya yang bertanda tangan dibawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh
/The undersigned, hereby declare that the scientific work written by

Nama /Name	: Millenito Nur Prasetiya
NIM /Student ID Number	: 41518120063
Program Studi /Study Program	: Teknik Informatika

Dengan Judul Tugas Akhir
/The title:
"Pemanfaatan Tools Security Information and Event Management (SIEM) dengan Autentikasi Indicator of Compromise (IoC) untuk Monitoring Perangkat bergerak pada lingkup jaringan internet perusahaan"
telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal:
/Similarity checks have been carried out with the Turnitin system on the date:

Kamis, 28 Agustus 2025

dengan nilai persentase sebesar :
/with a percentage value of:

6%

dinyatakan memenuhi standar sesuai dengan ketentuan berlaku di **Fakultas Ilmu Komputer** Universitas Mercu Buana. */declared to meet standards in accordance with applicable regulations at the Faculty of Computer Science, Universitas Mercu Buana.*

Jakarta, 28 Agustus 2025
Admin Turnitin Fasilkom UMB

Agung Prawoto

Agung Prawoto, S.Kom., B.Sc
NIK : 322970503

http://lib.mercubuana.ac.id
Menteng

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama	:	Millenito Nur Prasetiya
NIM	:	41518120063
Program Studi	:	Teknik Informatika
Judul Laporan Skripsi	:	Pemanfaatan SIEM dengan Autentikasi IoC untuk Monitoring Perangkat Bergerak di Jaringan Perusahaan.

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Laporan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 22 Agustus 2025

Yang menyatakan,



(Millenito Nur Prasetiya)

http://lib.mercubuana.ac.id
Menteng

HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh:

Nama	:	Millenito Nur Prasetiya
NIM	:	41518120063
Program Studi	:	Teknik Informatika
Judul Laporan Skripsi	:	Pemanfaatan SIEM dengan Autentikasi IoC untuk Monitoring Perangkat Bergerak di Jaringan Perusahaan.

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata 1 pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:

Pembimbing	:	Dwiki Jatikusumo,S.Kom.,M.Kom	
NIDN	:	0301128903	( )
Ketua Penguji	:	Hadi Santoso, Dr, S.Kom, M.Kom	
NIDN	:	0225067701	( )
Penguji 1	:	Siti Maesaroh, S.Kom., M.T.I	
NIDN	:	0413059003	( )
Penguji 2	:	Ida Farida, ST,M.Kom	
NIDN	:	0324018301	( )

Jakarta, 22 Agustus 2025
Mengetahui,

Dekan	Ketua Program Studi
Dr. Bambang Jokonowo, S.Si., MTI	Dr. Hadi Santoso, S.Kom., M.Kom
NIDN : 0320037002	NIDN : 0225067701

http://lib.mercubuana.ac.id
Menteng

KATA PENGANTAR

Puji syukur kehadirat Tuhan yang Maha Esa, atas segala rahmat dan ridha-Nya sehingga penulis dapat menyelesaikan tugas akhir yang merupakan salah satu persyaratan kelulusan Program Studi Strata Satu (S1) pada jurusan Teknik Informatika, Universitas Mercu Buana.

Penulis menyadari bahwa tugas akhir ini masih jauh dari sempurna, karena kesempurnaan sejatinya hanya milik Tuhan yang Maha Esa. Oleh karena itu, saran dan masukan yang membangun senantiasa penulis terima dengan senang hati. Serta berkat dukungan, motivasi, bantuan, bimbingan, dan doa dari banyak pihak, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana.
4. Bapak Dwiki Jatikusumo, S.Kom., M.Kom. selaku Dosen Pembimbing yang telah menyediakan waktu, tenaga dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini
5. Kedua Orang Tua saya yang selalu mensuport dan mendukung saya selama menjalani masa studi sebagai mahasiswa Universitas Mercubuana..
6. Semua teman kuliah yang selalu berbagi informasi dan memberikan dukungan dalam bentuk yang berbeda-beda.

Akhir kata, penulis berharap semoga Tuhan yang Maha Esa membalas kebaikan dan selalu mencurahkan rahmat, hidayah, serta panjang umur kepada kita semua, aamiin. Terima Kasih.

Jakarta, ……

Millenito Nur Prasetiya

http://lib.mercubuana.ac.id
Menteng

ABSTRAK

Nama	: Millenito Nur Prasetiya
NIM	: 41518120063
Program Studi	: Teknik Informatika
Judul Laporan Skripsi	: Pemanfaatan SIEM dengan Autentikasi IoC untuk Monitoring Perangkat Bergerak di Jaringan Perusahaan.
Dosen Pembimbing	: Bapak Dwiki Jatikusumo, S.Kom., M.Kom.

Penelitian ini membahas implementasi penggunaan perangkat lunak Security Information and Event Management (SIEM) yang terintegrasi dengan metode autentikasi berbasis Indicator of Compromise (IoC) sebagai upaya monitoring dan peningkatan keamanan terhadap perangkat bergerak yang terhubung dalam jaringan perusahaan. SIEM bertindak sebagai sistem terpusat dalam pengumpulan log, analisis, serta deteksi anomali pada jaringan, sementara IoC digunakan sebagai indikator teknis yang dapat mendeteksi potensi ancaman siber secara lebih cepat dan akurat. Penelitian ini menggunakan pendekatan studi kasus dengan pengujian pada lingkungan perusahaan yang memiliki perangkat mobile aktif, dan menilai efektivitas sistem berdasarkan parameter efisiensi, akurasi deteksi, dan kemudahan integrasi. Hasil dari penelitian ini menunjukkan bahwa integrasi SIEM dan IoC dapat meningkatkan kecepatan deteksi ancaman serta mengurangi risiko insiden keamanan secara signifikan.

Kata kunci: Security Information and Event Management (SIEM), Indicator of Compromise (IoC), Keamanan Jaringan, Monitoring, Perangkat Bergerak.

UNIVERSITAS MERCU BUANA

http://lib.mercubuana.ac.id
Menteng

ABSTRACT

Nama	: Millenito Nur Prasetiya
NIM	: 41518120063
Program Studi	: Teknik Informatika
Judul Laporan Skripsi	: Pemanfaatan SIEM dengan Autentikasi IoC untuk Monitoring Perangkat Bergerak di Jaringan Perusahaan.
Dosen Pembimbing	: Bapak Dwiki Jatikusumo, S.Kom., M.Kom.

This study discusses the implementation of Security Information and Event Management (SIEM) tools integrated with Indicator of Compromise (IoC)-based authentication methods as a solution for monitoring and enhancing the security of mobile devices connected to corporate networks. EM acts as a centralized system for log collection, analysis, and anomaly detection, while IoCs serve as technical indicators that enable faster and more accurate threat detection. This research employs a case study approach by testing in a corporate environment with active mobile devices, evaluating the system's effectiveness based on efficiency, detection accuracy, and integration simplicity. The results indicate that the integration of SIEM and IoC significantly improves threat detection speed and reduces the risk of security incidents.

Keywords: Security Information and Event Management (SIEM), Indicator of Compromise (IoC), Network Security, Monitoring, Mobile Devices.

MERCU BUANA

http://lib.mercubuana.ac.id
Menteng

DAFTAR ISI

HALAMAN JUDUL ..... **i**
HALAMAN PERNYATAAN ..... **ii**
HALAMAN SIMILARITY CHECK ..... **iii**
HALAMAN PENGESAHAN ..... **iv**
HALAMAN PERNYATAAN PUBLIKASI ..... **v**
KATA PENGANTAR ..... **vi**
ABSTRAK ..... **vii**
ABSTRACT ..... **viii**
DAFTAR ISI ..... **ix**
DAFTAR TABEL ..... **x**
DAFTAR GAMBAR ..... **xi**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Perumusan Masalah 3
1.3 Tujuan Penelitian 4
1.4 Manfaat Penelitian 5
1.5 Batasan Masalah 5
BAB II TINJAUAN PUSTAKA **6**
2.1 Penelitian Terdahulu 6
2.2 Teori Pendukung 8
BAB III METODE PENELITIAN **10**
3.1 Jenis Penelitian 10
3.2 Tahapan Penelitian 11
BAB IV HASIL & PEMBAHASAN **14**
BAB V KESIMPULAN DAN SARAN **20**
DAFTAR PUSTAKA **23**
LAMPIRAN **24**

UNIVERSITAS MERCU BUANA

http://lib.mercubuana.ac.id
Menteng

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait SIEM dan IoC……6
Tabel 3.4.1 Tools & Bahan Penelitian……...13
Tabel 4.1.1 Pengumpulan & Korelasi Log……14
Tabel 4.1.2 Integrasi Indicator of Compromise…….15
Tabel 4.1.3 Penjelasan Severity…….16
Tabel 4.2 Hasil Pengujian Sistem……..18
Tabel 4.3 Tabel Database Sistem……...18
Tabel 4.5 Kesesuaian Tujuan Penelitian…….19

UNIVERSITAS
MERCU BUANA

http://lib.mercubuana.ac.id
Menteng

DAFTAR GAMBAR

Gambar 3.2 Tahapan Penelitian……11
Gambar 3.4.2 Flow SIEM…….13
Gambar 4.1.1 Source IP Access Dashboard…….15
Gambar 4.1.2 Vulnerability Dashboard……16
Gambar 4.1.3 Malware Detection Dashboard……...17

UNIVERSITAS
MERCU BUANA

http://lib.mercubuana.ac.id
Menteng