IMPLEMENTASI WAZUH SIEM MONITORING UNTUK KEAMANAN INFRASTRUKTUR IT PADA PT GLOBAL INNOVATION TECHNOLOGY

LAPORAN MBKM MAGANG

SALWA PUTRI RISWANA
00000057092

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2025

IMPLEMENTASI WAZUH SIEM MONITORING UNTUK KEAMANAN INFRASTRUKTUR IT PADA PT GLOBAL INNOVATION TECHNOLOGY

LAPORAN MBKM MAGANG

SALWA PUTRI RISWANA
00000057092

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2025

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Salwa Putri Riswana
NIM	:	00000057092
Program Studi	:	Informatika

Menyatakan dengan sesungguhnya bahwa Laporan MBKM Magang saya yang berjudul:

IMPLEMENTASI WAZUH SIEM MONITORING UNTUK KEAMANAN INFRASTRUKTUR IT PADA PT GLOBAL INNOVATION TECHNOLOGY

merupakan hasil karya saya sendiri, bukan merupakan hasil plagiat, dan tidak pula dituliskan oleh orang lain; Semua sumber, baik yang dikutip maupun dirujuk, telah saya cantumkan dan nyatakan dengan benar pada bagian Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan karya ilmiah, saya bersedia menerima konsekuensi untuk dinyatakan TIDAK LULUS. Saya juga bersedia menanggung segala konsekuensi hukum yang berkaitan dengan tindak plagiarisme ini sebagai kesalahan saya pribadi dan bukan tanggung jawab Universitas Multimedia Nusantara.

Tangerang, 20 Januari 2025

(Salwa Putri Riswana)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Yang bertanda tangan di bawah ini:

Nama	:	Salwa Putri Riswana
NIM	:	00000057092
Program Studi	:	Informatika
Jenjang	:	S1
Jenis Karya	:	Magang

Menyatakan dengan sesungguhnya bahwa:

☑ Saya bersedia memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya di repositori Knowledge Center, sehingga dapat diakses oleh Civitas Akademika/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial dan saya juga tidak akan mencabut kembali izin yang telah saya berikan dengan alasan apapun.

☐ Saya tidak bersedia karena dalam proses pengajuan untuk diterbitkan ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*)**.

Tangerang, 20 Januari 2025

Yang menyatakan

Salwa Putri Riswana

** Jika tidak bisa membuktikan LoA jurnal/HKI selama enam bulan ke depan, saya bersedia mengizinkan penuh karya ilmiah saya untuk diunggah ke KC UMN dan menjadi hak institusi UMN.

Halaman Persembahan / Motto

”Live each day as if your life had just begun.”

Johann Wolfgang Von Goethe

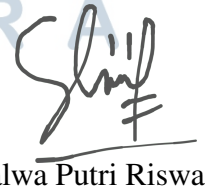
KATA PENGANTAR

Puji Syukur kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya, penulisan laporan Magang dengan judul: Implementasi Wazuh SIEM Monitoring untuk Keamanan Infrastruktur IT pada PT Global Innovation Technology dilakukan untuk memenuhi salah satu syarat mencapai gelar Sarjana Komputer Jurusan Informatika Universitas Multimedia Nusantara. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak dalam penyusunan laporan magang ini, sangatlah sulit bagi saya untuk menyelesaikan laporan magang ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Dr. Ir. Andrey Andoko, M.Sc., selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Bapak Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Ibu Marlinda Vasty Overbeek, S.Kom, M.Kom, sebagai Pembimbing pertama yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya tesis ini.
5. Bapak Ahmad Rizki selaku VP divisi *operation* di perusahaan PT Global Innovation Technology.
6. Kepada Orang Tua saya yang telah memberikan bantuan dukungan material dan moral sehingga penulis dapat menyelesaikan laporan magang ini.

Semoga laporan magang ini bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi bagi para pembaca.

Tangerang, 20 Januari 2025



Salwa Putri Riswana

IMPLEMENTASI WAZUH SIEM MONITORING UNTUK KEAMANAN INFRASTRUKTUR IT PADA PT GLOBAL INNOVATION TECHNOLOGY

Salwa Putri Riswana

ABSTRAK

Keamanan siber menjadi tantangan kritis di era digital, dengan meningkatnya kompleksitas serangan dan berkembangnya teknologi seperti IoT, cloud computing, dan perangkat mobile. Banyak organisasi masih menghadapi keterbatasan dalam memantau dan mendeteksi ancaman secara real-time, yang dapat membuat mereka rentan terhadap serangan yang tidak terdeteksi dalam waktu lama. Penelitian ini bertujuan untuk mengimplementasikan Wazuh sebagai platform Security Information and Event Management (SIEM) di PT Global Innovation Technology untuk meningkatkan keamanan sistem dan monitoring endpoint. Implementasi meliputi instalasi sistem, pembuatan dashboard security, dan integrasi alerting ke Telegram. Metode yang digunakan adalah pendekatan implementatif dengan fokus pada integrasi use case Security dan kustomisasi dashboard sesuai kebutuhan perusahaan. Hasil implementasi menunjukkan bahwa Wazuh berhasil memenuhi kriteria sebagai solusi keamanan siber yang komprehensif, dengan kemampuan monitoring SIEM yang efektif dan dapat disesuaikan dengan kebutuhan customer. Platform ini terbukti mampu memberikan visibilitas terhadap ancaman, mempercepat deteksi insiden, dan memberikan wawasan mendalam terkait keamanan jaringan. Implementasi ini diharapkan dapat menjadi solusi bagi permasalahan keamanan siber yang dihadapi customer PT Global Innovation Technology di masa mendatang.

Kata kunci: Wazuh, SIEM, Pemantauan Keamanan Sistem, Dashboard

IMPLEMENTATION OF WAZUH SIEM MONITORING FOR IT INFRASTRUCTURE SECURITY AT PT GLOBAL INNOVATION TECHNOLOGY

Salwa Putri Riswana

ABSTRACT

Cybersecurity has become a critical challenge in the digital era, with increasing attack complexity and evolving technologies such as IoT, cloud computing, and mobile devices. Many organizations still face limitations in monitoring and detecting threats in real-time, making them vulnerable to undetected attacks for extended periods. This research aims to implement Wazuh as a Security Information and Event Management (SIEM) platform at PT Global Innovation Technology to enhance system security and endpoint monitoring. The implementation includes system installation, security dashboard development, and Telegram alerting integration. The method used is an implementative approach focusing on Security use case integration and dashboard customization according to company requirements. Implementation results show that Wazuh successfully meets the criteria as a comprehensive cybersecurity solution, with effective SIEM monitoring capabilities that can be tailored to customer needs. The platform has proven capable of providing threat visibility, accelerating incident detection, and delivering deep insights into network security. This implementation is expected to serve as a solution for cybersecurity challenges faced by PT Global Innovation Technology's customers in the future.

***Keywords**: Wazuh, SIEM, Endpoint Security, Security Monitoring*

DAFTAR ISI

HALAMAN JUDUL i
PERNYATAAN TIDAK MELAKUKAN PLAGIAT ii
HALAMAN PERSETUJUAN PUBLIKASI ILMIAH iii
HALAMAN PERSEMBAHAN/MOTO iv
KATA PENGANTAR v
ABSTRAK vi
ABSTRACT vii
DAFTAR ISI viii
DAFTAR GAMBAR ix
DAFTAR TABEL xi
DAFTAR KODE xii
DAFTAR LAMPIRAN xiii
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Maksud dan Tujuan Kerja Magang 2
1.2.1 Maksud 2
1.2.2 Tujuan 2
1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang 3
BAB 2 GAMBARAN UMUM PERUSAHAAN 4
2.1 Sejarah Singkat Perusahaan 4
2.2 Visi dan Misi Perusahaan 4
2.2.1 Visi 4
2.2.2 Misi 4
2.3 Struktur Organisasi Perusahaan 5
BAB 3 PELAKSANAAN KERJA MAGANG 7
3.1 Kedudukan dan Organisasi 7
3.2 Tugas yang Dilakukan 7
3.3 Uraian Pelaksanaan Magang 8
3.3.1 Ancaman Siber (*Cyber Threat)* 9
3.3.2 Wazuh 12
3.4 Hasil dan Implementasi 15
3.4.1 Instalasi dan Konfigurasi Komponen Wazuh 15
3.4.2 Pembuatan Dashboard 18
3.4.3 Integrasi Alert Wazuh Via Telegram 48
3.5 Kendala dan Solusi yang Ditemukan 54
3.5.1 Kendala Yang Ditemukan 54
3.5.2 Solusi 55
BAB 4 SIMPULAN DAN SARAN 56
4.1 Simpulan 56
4.2 Saran 56
DAFTAR PUSTAKA 58

DAFTAR GAMBAR

Gambar 2.1 Struktur organisasi perusahaan PT GIT 5
Gambar 3.1 Komponen Wazuh 13
Gambar 3.2 Dashboard Autentikasi 19
Gambar 3.3 Panel total *authentication failed* 20
Gambar 3.4 Panel total *authentication success* 20
Gambar 3.5 Panel jumlah *agent* yang aktif 20
Gambar 3.6 Panel jumlah percobaan akses yang tidak valid 20
Gambar 3.7 Panel daftar tabel *agent* 21
Gambar 3.8 Panel yang berisi informasi akses *user* 21
Gambar 3.9 Panel berbentuk *maps* lokasi yang mencoba akses 21
Gambar 3.10 Panel yang menunjukkan list *user* yang mengakses 22
Gambar 3.11 Panel yang menunjukkan list IP *Address* yang mencoba akses 22
Gambar 3.12 Panel yang menunjukkan list *agent* dengan keterangan jumlahnya 22
Gambar 3.13 Dashboard Anomali Akses 23
Gambar 3.14 Metrik utama *Access Anomalies Dashboard* 24
Gambar 3.15 Panel dashboard Mitre Technique 24
Gambar 3.16 Panel *maps* informasi serangan *brute force* 25
Gambar 3.17 Panel dashboard informasi IP *Address* yang mencoba melakukan *brute force* 25
Gambar 3.18 Kelompok panel dashboard *IP Anomalies Gantt Chart* . . 26
Gambar 3.19 Panel dashboard grafik Mitre Technique 26
Gambar 3.20 Panel dashboard grafik IP *brute force* 27
Gambar 3.21 Panel dashboard grafik IP *Failed Login* 27
Gambar 3.22 Dashboard *Monitoring* Database 28
Gambar 3.23 Panel dashboard aktivitas database 28
Gambar 3.24 Panel dashboard *timestamp* aktivitas database 29
Gambar 3.25 Panel dashboard aktivitas *user* dari database 29
Gambar 3.26 Panel dashboard aktivitas terkini dari database 29
Gambar 3.27 Dashboard VirusTotal 30
Gambar 3.28 Panel dashboard total dilakukan pemindaian 30
Gambar 3.29 Panel dashboard positif virus terdeteksi 31
Gambar 3.30 Panel dashboard pemindaian dengan hasil negatif adanya virus 31
Gambar 3.31 Panel dashboard dengan detail informasi terkait virus . . . 32
Gambar 3.32 Panel dashboard grafik jumlah virus positif tercatat 32
Gambar 3.33 Dashboard Vulnerability 33
Gambar 3.34 Panel *Low Severity* 34
Gambar 3.35 Panel *Medium Severity* 34
Gambar 3.36 Panel *High Severity* 35
Gambar 3.37 Panel *Critical Severity* 35
Gambar 3.38 Panel tabel CVE *Code Information* 36
Gambar 3.39 Panel tabel Top 5 *Agents* 36
Gambar 3.40 Panel tabel *Package* 37
Gambar 3.41 Panel tabel informasi detail terkait kerentanan sistem . . . 37

Gambar 3.42 Panel tabel informasi mencakup nama *endpoint*, nama *package* dan kode CVE serta versi dari *package* 38
Gambar 3.43 Panel tabel informasi detail terkait kerentanan sistem . . . 38
Gambar 3.44 Dashboard Deteksi Malware 39
Gambar 3.45 Panel tipe malware 39
Gambar 3.46 Panel malware terdeteksi 40
Gambar 3.47 Panel malware yang sudah dilakukan mitigasi 40
Gambar 3.48 Panel respon dari AI terkait malware yang terdeteksi . . . 41
Gambar 3.49 Panel tabel detail dari YARA 41
Gambar 3.50 Dashboard Eksekutif 42
Gambar 3.51 Panel dashboard utama dalam *Executive* Dashboard 42
Gambar 3.52 Panel dashboard jumlah akses gagal 43
Gambar 3.53 Panel dashboard informasi jumlah *malware* yang terdeteksi 43
Gambar 3.54 Panel dashboard jumlah file berbahaya terdeteksi 43
Gambar 3.55 Panel dashboard jumlah kerentanan *critical* terdeteksi . . . 44
Gambar 3.56 Panel dashboard jumlah *user* melakukan **DROP** 44
Gambar 3.57 Panel dashboard jumlah kerentanan yang belum dilakukan *solving* 45
Gambar 3.58 Kelompok panel dashboard *authentication* 45
Gambar 3.59 Panel dashboard *top 5 agent* 45
Gambar 3.60 Panel dashboard lokasi percobaan akses gagal 46
Gambar 3.61 Panel dashboard informasi malware 46
Gambar 3.62 Panel dashboard tipe malware 47
Gambar 3.63 Panel dashboard agent yang terdeteksi ada malware 47
Gambar 3.64 Panel dashboard *database monitoring* 48
Gambar 3.65 Panel dashboard *malicious hash file* 48
Gambar 3.66 *Command* untuk membuat Bot 49
Gambar 3.67 Memasukkan nama Bot 49
Gambar 3.68 Bot berhasil dibuat 50
Gambar 3.69 Respon API saat dikirimkan *chat* 51
Gambar 3.70 Skrip *custom-telegram* berada di direktori 53
Gambar 3.71 File sudah diubah hak akses dan kepemilikannya 53
Gambar 3.72 Konfigurasi integrasi Telegram di *ossec.conf* 53
Gambar 3.73 Tampilan *alert* otomatis yang sudah berhasil masuk 54

DAFTAR TABEL

Tabel 3.1 Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang 8

DAFTAR KODE

3.1 Skrip *Python* integrasi Wazuh - Telegram 51

DAFTAR LAMPIRAN

Lampiran 1 MBKM-01 Cover Letter MBKM Internship Track 1 59
Lampiran 2 MBKM-02 MBKM Internship Track 1 Card 60
Lampiran 3 MBKM-03 Daily Task - Internship Track 1 61
Lampiran 4 MBKM-04 Verification Form of Internship Report MBKM Internship Track 1 62
Lampiran 5 Form Bimbingan 63
Lampiran 6 Hasil Turnitin 64