IMPLEMENTASI FRAMEWORK MITRE ATT&CK UNTUK DETEKSI ANCAMAN SIBER PADA SOC L1 PT DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

ALVIANDA CHAIROFTA
00000082435

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

IMPLEMENTASI FRAMEWORK MITRE ATT&CK UNTUK DETEKSI ANCAMAN SIBER PADA SOC L1 PT DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

ALVIANDA CHAIROFTA
00000082435

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG
2025

HALAMAN PERNYATAAN ORISINALITAS TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Alvianda Chairofta
NIM	:	00000082435
Program Studi	:	Informatika

Menyatakan dengan sesungguhnya bahwa Laporan MBKM Magang saya yang berjudul:

Implementasi Framework MITRE ATT&CK untuk Deteksi Ancaman Siber pada SOC L1 PT Defender Nusa Semesta

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 Juni 2025

(Alvianda Chairofta)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH MAHASISWA

Yang bertanda tangan di bawah ini:

Nama	:	Alvianda Chairofta
NIM	:	00000082435
Program Studi	:	Informatika
Jenjang	:	S1
Jenis Karya	:	Laporan MBKM 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 Juni 2025

Yang menyatakan

Alvianda Chairofta

** 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

”Hey boy, keep running!”

Ryan Gosling

KATA PENGANTAR

Mengucapkan terima kasih

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. Bapak Yustinus Widya Wiratama, S.Kom., M.Sc., sebagai Pembimbing pertama yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya laporan ini.
5. Kepada Bapak Andi Wahyudi selaku Tim Leader *Security Operation Center (SOC)* PT Defender Nusa Semesta sekaligus Site Supervisor, atas kesempatan, kepercayaan, dan dukungan yang telah diberikan kepada penulis selama menjalani program magang di perushaan.
6. Kepada Talbyahya Herdy Putra selaku *Buddy*, yang telah membantu adaptasi penulis dan berkembang selama program magang berlangsung.
7. Kepada seluruh rekan kerja di PT Defender Nusa Semesta, yang telah memberikan bantuan dan dukungan selama proses magang dan penyusunan laporan ini.
8. Kedua orang tua dan seluruh keluarga penulis atas segala dukungan baik secara material dan moral, sehingga penulis, yang menjadi motivasi penulis dalam menyelesaikan laporan ini.

Semoga karya ilmiah ini bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi, bagi para pembaca.

Tangerang, 20 Juni 2025

Alvianda Chairofta

IMPLEMENTASI FRAMEWORK MITRE ATT&CK UNTUK DETEKSI ANCAMAN SIBER PADA SOC L1 PT DEFENDER NUSA SEMESTA

Alvianda Chairofta

ABSTRAK

Seiring dengan meningkatnya kompleksitas ancaman siber, organisasi memerlukan pendekatan yang terstruktur untuk mendeteksi dan merespons insiden keamanan. Laporan magang ini membahas implementasi praktis *framework MITRE ATT&CK* sebagai basis pengetahuan untuk deteksi ancaman di lingkungan *Security Operations Center (SOC) Level 1 (L1)* PT Defender Nusa Semesta. Melalui kegiatan magang sebagai Security Analyst, dilakukan analisis mendalam terhadap studi kasus anomali eksekusi *regsvr32.exe* yang terdeteksi pada sistem salah satu customer. Proses analisis mencakup identifikasi case melalui Security Information and Event Management (SIEM), investigasi dan korelasi log dari berbagai perangkat keamanan seperti Wazuh HIDS dan Trend Micro, hingga pemetaan aktivitas ancaman ke dalam taktik dan teknik (TTP) pada *framework MITRE ATT&CK*. Hasil analisis berhasil mengidentifikasi beberapa TTP yang digunakan penyerang, antara lain *Execution (T1218.007: Regsvr32), Persistence (T1547.001: Registry Run Keys / Startup Folder)*, dan *Command and Control (T1071.001: Web Protocols)*. Implementasi ini membuktikan bahwa *MITRE ATT&CK* sangat efektif dalam menindaklanjuti, menstandarisasi proses analisis, dan mempercepat respons insiden secara tepat.

Keywords: Deteksi Ancaman, Keamanan Siber, *MITRE ATT&CK*, *Security Operations Center (SOC)*

IMPLEMENTATION OF THE MITRE ATTCK FRAMEWORK FOR CYBER THREAT DETECTION IN THE SOC L1 OF PT DEFENDER NUSA SEMESTA

Alvianda Chairofta

ABSTRACT

As cyber threats continue to grow in complexity, organizations require a structured approach to effectively detect and respond to security incidents. This internship report discusses the practical implementation of the MITRE ATTCK framework as a knowledge base for threat detection within the Security Operations Center (SOC) Level 1 (L1) at PT Defender Nusa Semesta. During the internship as a Security Analyst, an in-depth analysis was conducted on a case involving anomalous execution of regsvr32.exe detected on a customer's system. The analysis process included case identification via the Security Information and Event Management (SIEM) platform, log investigation and correlation from various security tools such as Wazuh HIDS and Trend Micro, and mapping threat activities to tactics, techniques, and procedures (TTPs) within the MITRE ATTCK framework. The analysis successfully identified several TTPs used by the attacker, including Execution (T1218.007: Regsvr32), Persistence (T1547.001: Registry Run Keys / Startup Folder), and Command and Control (T1071.001: Web Protocols). This implementation demonstrates that MITRE ATTCK is highly effective in facilitating incident response, standardizing the analysis process, and accelerating accurate threat mitigation.

Keywords: *Cybersecurity, MITRE ATT&CK, Security Operations Center (SOC), Threat Detection*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN