PENERAPAN EDR (*ENDPOINT DETECTION RESPONSE*) DAN MVM (*MANAGED VULNERABILITY MANAGEMENT*) UNTUK PENCEGAHAN *CYBER ATTACK* (STUDI KASUS YAYASAN DHARMA BHAKTI ASTRA)

LAPORAN TUGAS AKHIR

MUHAMMAD WAHYUDIN WISESAR

41519110028

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2025

PENERAPAN EDR *(ENDPOINT DETECTION RESPONSE)* DAN MVM *(MANAGED VULNERABILITY MANAGEMENT)* UNTUK PENCEGAHAN *CYBER ATTACK* (STUDI KASUS YAYASAN DHARMA BHAKTI ASTRA)

LAPORAN TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

MUHAMMAD WAHYUDIN WISESAR
41519110028

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

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama	: Muhammad Wahyudin Wisesar
NIM	: 41519110028
Program Studi	: Teknik Informatika
Judul Proposal Penelitian	: Penerapan EDR (*Endpoint Detection Response*) Dan MVM (*Managed Vulnerability Management*) Untuk Pencegahan *Cyber Attack* (Studi Kasus Yayasan Dharma Bhakti Astra)

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

Jakarta, 3 Februari 2025

(Muhammad Wahyudin Wisesar)

HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh:

Nama : Muhamad Wahyudin Wisesar

NIM : 41519110028

Program Studi : Teknik Informatika

Judul Laporan Skripsi : Penerapan EDR (*Endpoint Detection Response*) Dan MVM (*Managed Vulnerability Management*) Untuk Pencegahan *Cyber Attack* (Studi Kasus Yayasan Dharma Bhakti Astra)

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 : Muhammad Rifqi, S.Kom., M.Kom. ( )

NIDN : 0301067101

Ketua Penguji : Wawan Gunawan, S.Kom., M.T. ( )

NIDN : 0424108104

Penguji 1 : Roy Mubarak, S.T., M.Kom. ( )

NIDN : 0310027402

Penguji 2 : Sabar Rudiarto, S.Kom., M.Kom. ( )

NIDN : 0309036902

Jakarta, 3 Februari 2025

Mengetahui,

Dekan	Ketua Program Studi
Dr. Bambang Jokonowo, S.Si., M.T.I	Dr. Hadi Santoso, S.Kom,M.Kom
0327097207	0225067701

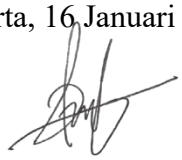
KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat- Nya, saya dapat menyelesaikan Proposal Penelitian ini. Penulisan Proposal Penelitian ini dilakukan dalam rangka memenuhi salah satu syarat untuk disidangkan pada seminar proposal. Saya menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan Proposal Penelitian ini, sangatlah sulit bagi saya untuk menyelesaikan Laporan Tugas Akhir. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng selaku Rektor Universitas Mercu Buana Jakarta.
2. Bapak Dr. Bambang Jokonowo, S.Si., M.T.I selaku Dekan Fakultas Ilmu Komputer Universitas Mercu Buana Jakarta.
3. Bapak Dr. Hadi Santoso, S.Kom,M.Kom, selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana Jakarta.
4. Bapak Muhammad Rifqi Pasani M.Kom selaku Dosen Pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan laporan tugas akhir.
5. Saudari Lim Xiao Yin sebagai sumber dukungan dan semangat penulis dalam menyelesaikan laporan tugas akhir ini.
6. Saudara Reza Firgiyanto selaku teman seperjuangan akademik yang selalu menjadi teman diskusi selama menempuh studi akademik di Universitas Mercu Buana.
7. Saudara Alfredo Wijaya, S.Ked selaku teman diskusi selama menyelesaikan laporan tugas akhir ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Proposal Penelitian ini dapat membawa manfaat bagi pengembangan ilmu pengetahuan.

Jakarta, 16 Januari 2025



Muhammad Wahyudin Wisesar

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama	: Muhamad Wahyudin Wisesar
NIM	: 41519110028
Program Studi	: Teknik Informatika
Judul Laporan Skripsi	: Penerapan EDR (*Endpoint Detection Response*) Dan MVM (*Managed Vulnerability Management*) Untuk Pencegahan *Cyber Attack* (Studi Kasus Yayasan Dharma Bhakti Astra)

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 Magang/Skripsi/Tesis/Disertasi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 3 Februari 2025

Yang menyatakan,

(Muhamad Wahyudin Wisesar)

ABSTRAK

Nama	: Muhammad Wahyudin Wisesar
NIM	: 41519110028
Program Studi	: Teknik Informatika
Judul Proposal Penelitian	: Penerapan EDR (*Endpoint Detection Response*) Dan MVM (*Managed Vulnerability Management*) Untuk Pencegahan *Cyber Attack* (Studi Kasus Yayasan Dharma Bhakti Astra)
Pembimbing	: Muhammad Rifqi Pasani, M.Kom

Keamanan siber saat ini merupakan aspek yang sangat penting dalam dunia yang semakin terhubung secara digital. Artikel ini menggambarkan kondisi keamanan siber saat ini dengan fokus pada perubahan dan tantangan terkini. Ancaman siber semakin canggih, melibatkan serangan malware yang mutakhir, peretasan jaringan yang kompleks, dan kampanye phishing yang lebih licik. Keamanan siber saat ini juga diwarnai oleh serangan siber negara dan peningkatan aktivitas siber-kriminalitas.

Endpoint Detection and Response (EDR) adalah pendekatan penting dalam keamanan siber yang fokus pada deteksi dan respons terhadap ancaman siber pada tingkat *Endpoint* dalam jaringan komputer. Dengan menggunakan teknik analisis perilaku dan kecerdasan buatan, EDR memungkinkan organisasi untuk mendeteksi ancaman siber yang mungkin terlewatkan oleh alat keamanan konvensional. EDR juga memungkinkan respons yang cepat dan isolasi *Endpoint* terinfeksi, membantu melindungi sistem dan data dari serangan siber. Artikel ini merangkum konsep dasar EDR, manfaatnya, dan perannya dalam strategi keamanan siber modern.

Managed Vulnerability Management (MVM) adalah perangkat yang penting dalam upaya melindungi infrastruktur IT dari serangan siber dengan mengidentifikasi, menilai, dan mengelola kerentanan yang ada. MVM membantu organisasi dalam mengurangi risiko dengan mengatasi kerentanan yang dapat dieksploitasi oleh penyerang, sehingga menjaga keamanan sistem dan data,

identifikasi kerentanan, manajemen risiko, pemantauan berkelanjutan, dan peran MVM dalam mematuhi regulasi keamanan. Dengan perangkat MVM yang efektif, organisasi dapat meminimalkan risiko dan mempertahankan integritas infrastruktur IT organisasi atau perusahaan tersebut.

Kata Kunci: Keamanan Siber, EDR, MVM, Serangan Siber, SOC

ABSTRACT

Name	: Muhamad Wahyudin Wisesar
NIM	: 41519110028
Study Program	: Informatics Engineering
Tittle Thesis	: Implementation of EDR (Endpoint Detection Response) and MVM (Managed Vulnerability Management) to Prevent Cyber Attacks (Case Study of the Dharma Bhakti Astra Foundation)
Counsellor	: Muhammad Rifqi Pasani, M.Kom

Cybersecurity has become a critical aspect in an increasingly interconnected digital world. This article highlights the current state of cybersecurity, focusing on the latest changes and challenges. Cyber threats have grown more sophisticated, involving advanced malware attacks, complex network breaches, and more cunning phishing campaigns. The cybersecurity landscape is also marked by state-sponsored cyberattacks and the rise of cybercriminal activities.

Endpoint Detection and Response (EDR) Endpoint Detection and Response (EDR) is a crucial approach in cybersecurity, focusing on detecting and responding to cyber threats at the endpoint level within a computer network. By leveraging behavioral analysis techniques and artificial intelligence, EDR enables organizations to detect cyber threats that might be overlooked by conventional security tools. EDR also facilitates swift responses and isolates infected endpoints, helping protect systems and data from cyberattacks. This article summarizes the fundamental concepts of EDR, its benefits, and its role in modern cybersecurity strategies.

Managed Vulnerability Management (MVM) Managed Vulnerability Management (MVM) is a vital tool in protecting IT infrastructure from cyberattacks by identifying, assessing, and managing existing vulnerabilities. MVM helps organizations reduce risks by addressing vulnerabilities that attackers could exploit, thereby safeguarding systems and data. This includes vulnerability identification,

risk management, continuous monitoring, and MVM's role in complying with security regulations. With effective MVM tools, organizations can minimize risks and maintain the integrity of their IT infrastructure.

Keywords : Cyber Security, EDR, MVM, Cyber Attack, SOC

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN