Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
https://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/index
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893

Implementasi Kerangka Kerja MITRE D3FEND dalam Mitigasi Serangan Ransomware LockBit 3.0

DOI: http://dx.doi.org/10.35889/jutisi.v15i3.3636

Syahbagus Raditya Haryo Santoso[1], Henni Endah Wahanani[2*], Achmad Junaidi[3]
Informatika, Universitas Pembangunan Nasional Veteran Jawa Timur, Surabaya, Indonesia
*e-mail *Corresponding Author:* henniendah.if@upnjatim.ac.id

Abstract

Cybersecurity threats are escalating due to the evolution of LockBit 3.0 ransomware, which has disrupted national vital sectors. This study aims to demonstrate the implementation of the MITRE D3FEND framework to mitigate these attacks within a Windows 11 environment. An experimental method using a technical comparative analysis approach was applied and validated through 50 test iterations to ensure data reliability. The results indicate that the baseline unprotected system is completely vulnerable to the entire LockBit 3.0 attack chain. However, the deployment of MITRE D3FEND controls proactively enhances system resilience, achieving a 75% effectiveness score by successfully executing passive detection and real-time active blocking at critical attack vectors. This study concludes that a digital artifact-based defense strategy significantly hardens cyber infrastructure, while recommending future developments in artificial intelligence (AI) based adaptive mitigation automation.

Kata kunci: *MITRE D3FEND; LockBit 3.0; Cybersecurity; Ransomware; Mitigation*

Abstrak

Ancaman keamanan siber meningkat akibat evolusi ransomware LockBit 3.0 yang melumpuhkan berbagai sektor vital nasional. Penelitian ini bertujuan mendemonstrasikan implementasi kerangka kerja MITRE D3FEND dalam memitigasi serangan tersebut pada Windows 11. Metode eksperimen diterapkan melalui pendekatan analisis komparatif teknis yang divalidasi lewat 50 kali iterasi pengujian guna menjamin reliabilitas data. Hasil pengujian menunjukkan bahwa sistem standar tanpa proteksi sepenuhnya rentan terhadap seluruh rangkaian serangan LockBit 3.0. Namun, penerapan kontrol pertahanan MITRE D3FEND terbukti proaktif meningkatkan resiliensi sistem dengan skor efektivitas mencapai 75% melalui keberhasilan fungsi deteksi pasif serta pemblokiran aktif secara real-time di titik-titik krusial serangan. Penelitian ini menyimpulkan bahwa strategi pertahanan berbasis artefak digital secara signifikan memperkeras keamanan infrastruktur siber, sekaligus merekomendasikan pengembangan otomatisasi mitigasi adaptif berbasis kecerdasan buatan (AI) di masa depan.

Kata kunci: *MITRE D3FEND; LockBit 3.0; Cybersecurity; Ransomware; Mitigasi*

1. Pendahuluan

Keamanan siber saat ini menghadapi ancaman yang sangat serius dari serangan ransomware, yang secara konsisten menargetkan ketersediaan data dan kelumpuhan infrastruktur kritis di berbagai sektor [1]. Salah satu ancaman paling mendominasi dalam lanskap ini adalah LockBit 3.0, yang juga dikenal sebagai LockBit Black [2]. Beroperasi melalui ekosistem *Ransomware-as-a-Service* (RaaS), LockBit 3.0 dikenal memiliki tingkat destruksi yang tinggi karena kecepatannya dalam mengenkripsi file, serta kemampuannya yang berevolusi menggunakan skema pemerasan ganda [3]. Eskalasi serangan dari varian ini telah banyak melumpuhkan sektor vital secara global. Di Indonesia, dampak destruktif ini terlihat nyata pada insiden yang melumpuhkan sektor perbankan nasional melalui serangan terhadap Bank Syariah Indonesia (BSI) pada 2023 [4]. Namun, eskalasi ancaman mencapai puncaknya pada Juni 2024, di mana varian LockBit 3.0 melumpuhkan layanan di lebih dari 210 institusi pemerintah melalui serangan terhadap Pusat Data Nasional Sementara (PDNS), yang menegaskan bahwa

infrastruktur informasi vital nasional masih memiliki celah keamanan yang signifikan terhadap evolusi ransomware [5]. Fenomena ini menuntut adanya pendekatan pertahanan siber yang jauh lebih tangguh dibandingkan sekadar mengandalkan pemindaian perangkat lunak antivirus tradisional.

Tuntutan akan sistem pertahanan yang lebih tangguh tersebut muncul bukan tanpa alasan, melainkan karena kompleksitas dari serangan LockBit 3.0 yang terletak pada penggunaan taktik yang sangat adaptif dan tersembunyi [2]. Alih-alih langsung mengenkripsi data saat berhasil menyusup, LockBit 3.0 melakukan serangkaian manuver eksploitasi yang menyerupai aktivitas normal di dalam sistem [6]. Rantai serangan ini umumnya meliputi pencurian kredensial (*Credential Access*) menggunakan utilitas pihak ketiga, penyebaran infeksi secara masif ke mesin lain melalui layanan jaringan *Server Message Block* (SMB), hingga melakukan sabotase dengan melumpuhkan alat keamanan bawaan sistem operasi (*Impair Defenses*) [7]. Karena pergerakan ini sangat menyatu dengan penggunaan alat administrasi sistem yang sah (*living off the land*), ancaman sering kali lolos dari deteksi [6]. Oleh karena itu, diperlukan validasi empiris terhadap kerangka kerja defensif yang mampu beroperasi pada level artefak digital guna mendeteksi anomali perilaku sebelum dampak destruktif terjadi [8].

Berbagai literatur terdahulu sesungguhnya telah berupaya menjawab tantangan mitigasi ransomware ini melalui beragam pendekatan teknis maupun manajerial. Pada ranah analisis ofensif (Red Team), Eliando dan Warsito [4] melakukan dekonstruksi terhadap metode infeksi LockBit melalui *reverse shell*, yang kemudian diperdalam oleh Suk-on pada tahun 2024 [2], melalui investigasi forensik digital untuk mempelajari gerakan dari malware di infrastruktur operasional. Selain itu, Lanza [9] mengoptimalkan ekstraksi intelijen ancaman untuk mengklasifikasikan taktik penyerang secara presisi. Dari sisi pertahanan (Blue Team), Mavire [1] membuktikan efektivitas strategi pertahanan berlapis, sementara Li dan Madisetti [8] mengembangkan sistem ERAD (*Enhanced Ransomware Attack Defense*) yang memanfaatkan pemetaan *Indicators of Compromise* (IOC) guna memberikan rekomendasi tindakan balasan spesifik. Kajian Syifa dan Salman [10] turut memperkuat pemahaman mengenai interaksi dinamis keamanan dan evaluasi vektor serangan menggunakan Cyber Kill Chain. Upaya menjembatani celah teknis melalui kerangka kerja MITRE juga dikembangkan, di mana penelitian oleh Husseis [11] membuktikan penggunaan matriks ATT&CK dalam meningkatkan pengambilan keputusan proaktif. Lebih jauh, Hasan [12] mengusulkan integrasi pemodelan ofensif ATT&CK dengan kapabilitas defensif D3FEND guna mengidentifikasi celah keamanan secara terarah, sementara Oliveira berfokus pada standardisasi taktik melalui analisis ontologi D3FEND. Pendekatan ini dilengkapi oleh Mohamed [13] yang memanfaatkan kerangka kerja tersebut untuk memprioritaskan strategi mitigasi berdasarkan pengambilan keputusan multikriteria. Meskipun riset-riset tersebut membangun fondasi yang kuat, masih terdapat celah yang signifikan dalam aspek pembuktian empiris, mengingat bahwa pendekatan saat ini umumnya masih berkutat pada panduan manajerial, terbatas pada pemodelan teoretis, atau sebatas melakukan analisis pasca-insiden tanpa memvalidasi secara teknis efektivitas kontrol mitigasi pada level modifikasi artefak digital secara dinamis di lingkungan sistem operasi nyata.

Berangkat dari celah literatur yang masih didominasi oleh kebijakan manajerial dan konseptual teoretis tersebut, penelitian ini mengambil langkah lebih jauh dengan mendemonstrasikan implementasi teknis kerangka kerja MITRE D3FEND untuk menanggulangi eksekusi LockBit 3.0 secara langsung di dalam lingkungan target operasi. Secara rasional, D3FEND dipandang sebagai solusi yang sangat efektif untuk menutup celah tersebut karena kerangka ini tidak beroperasi pada tatanan kebijakan makro, melainkan bekerja secara langsung pada level "artefak digital" sistem seperti modifikasi *registry*, proses eksekusi *file*, dan lalu lintas jaringan. Melalui intervensi pada artefak digital inilah, wawasan ancaman yang teoretis dapat diterjemahkan menjadi langkah mitigasi otomatis secara teknis, baik melalui taktik memperkeras konfigurasi OS (*Harden*), mendeteksi anomali secara *real-time* (*Detect*), maupun mengisolasi proses dan lingkungan jaringan (*Isolate*) [14]. Letak perbedaan mendasar serta kontribusi utama dari kajian ini muncul melalui pergeseran paradigma dari sekadar analisis ancaman yang pasif menuju aksi defensif teknis yang nyata. Dengan melakukan pembuktian empiris di lingkungan sistem operasi modern, riset ini akan memastikan konfigurasi pertahanan berbasis artefak mana yang paling optimal untuk melumpuhkan manuver LockBit 3.0, sekaligus menghasilkan sebuah cetak biru (*blueprint*) arsitektural yang tangguh bagi praktisi keamanan siber di lapangan.

2. Metodologi

Bab ini menyajikan kerangka metodologis dan teknis yang digunakan untuk mengevaluasi kapabilitas mitigasi dari kerangka kerja MITRE D3FEND terhadap serangan ransomware LockBit 3.0. Fokus utama dari bab ini adalah menguraikan rancangan eksperimen di lingkungan laboratorium virtual, prosedur penyiapan skenario serangan, serta metode analisis yang diterapkan untuk mengukur tingkat efektivitas pertahanan secara objektif dan terukur.

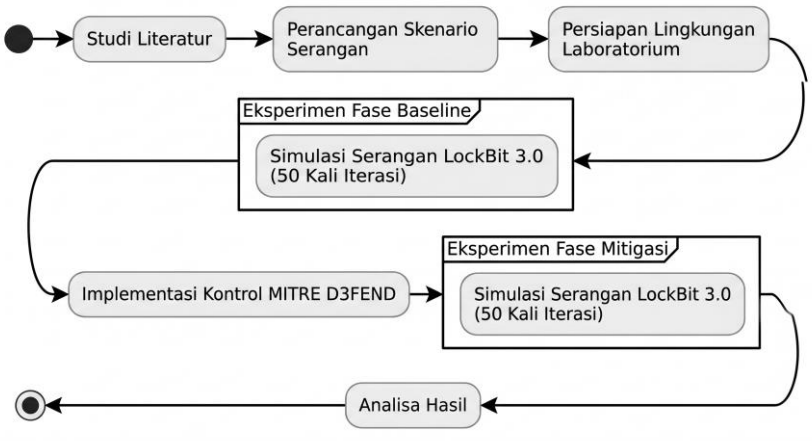
2.1 Metode Penelitian dan Alur Eksperimen

Penelitian ini menerapkan metode eksperimen dengan pendekatan analisis komparatif teknis untuk mengevaluasi kemampuan mitigasi kerangka kerja pertahanan siber. Penggunaan lingkungan *virtual machine* (VM) menjadi instrumen utama karena memungkinkan terciptanya ekosistem yang terisolasi dari infrastruktur nyata, sehingga simulasi serangan dapat dilakukan secara aman dengan kondisi yang dapat dikontrol sepenuhnya. Variabel utama dalam penelitian ini adalah penerapan konfigurasi pertahanan berbasis MITRE D3FEND yang diukur terhadap respon sistem saat menghadapi teknik serangan ransomware LockBit 3.0. Untuk memperoleh data yang valid, penelitian ini menyertakan kondisi *baseline* rentan sebagai titik pembanding awal untuk melihat sejauh mana sistem dapat ditembus tanpa adanya intervensi kontrol keamanan.

Secara sistematis, alur penelitian ini dimulai dengan tahap studi literatur untuk memahami karakteristik teknis LockBit 3.0 dan fungsionalitas kerangka kerja MITRE D3FEND. Setelah pemahaman teoritis terpenuhi, dilakukan perancangan skenario serangan menggunakan matriks MITRE ATT&CK yang kemudian diikuti dengan persiapan lingkungan laboratorium virtual. Proses pengujian dilaksanakan dalam dua fase utama, yaitu uji *baseline* untuk mendokumentasikan dampak serangan pada sistem standar tanpa proteksi, dan uji mitigasi untuk menganalisis pertahanan sistem setelah penerapan kontrol D3FEND. Perbandingan antara kedua fase ini digunakan untuk memberikan bukti teknis yang mendalam mengenai bagaimana setiap tahapan dalam rantai serangan berhasil dideteksi atau dihentikan secara efektif.

2.2 Alur Penelitian

Pelaksanaan penelitian ini mengikuti peta jalan yang dirancang untuk menjamin keterukuran hasil di setiap fasenya. Alur ini tidak hanya sekadar urutan kerja, melainkan sebuah kerangka berpikir yang menjembatani identifikasi teoritis mengenai perilaku LockBit 3.0 dengan pembuktian teknis di laboratorium virtual. Dengan mengadopsi prosedur yang sistematis, setiap temuan dalam eksperimen dapat dipertanggungjawabkan secara ilmiah, mulai dari tahap pemetaan artefak digital hingga proses ekstraksi data hasil mitigasi. Representasi visual dari metodologi dan tahapan operasional tersebut dipetakan dalam diagram alur penelitian pada Gambar 1.



Gambar 1. Alur Penelitian

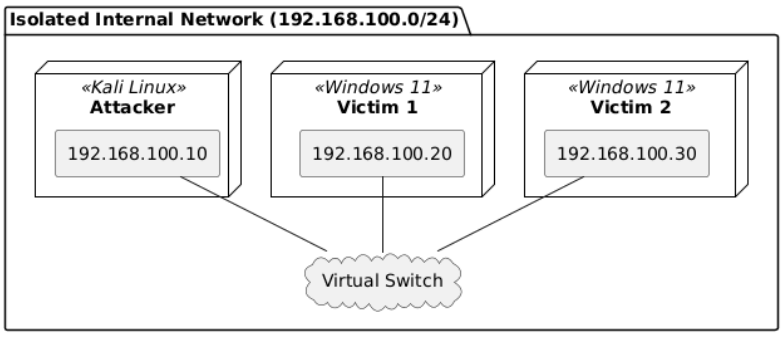
Gambar 1 di atas mengilustrasikan alur eksperimen yang disusun secara sistematis dan komprehensif. Tahapan penelitian diawali dengan studi literatur dan dekonstruksi terhadap TTP LockBit 3.0 guna memetakan vektor serangan yang akan menjadi target intervensi pertahanan.

Inti dari rangkaian metodologi ini terletak pada fase pengujian komparatif yang dilakukan melalui 50 kali iterasi untuk setiap skenario.

Sistem dievaluasi melalui dua kondisi yang berbeda, fase *baseline* untuk mendokumentasikan dampak serangan tanpa proteksi, dan fase mitigasi untuk memverifikasi efektivitas kontrol D3FEND setelah diimplementasikan. Pendekatan perbandingan langsung dengan jumlah pengulangan yang tinggi ini sangat krusial untuk memverifikasi hubungan sebab-akibat antara penerapan kontrol dengan hasil mitigasi secara konsisten. Dengan demikian, setiap respon seperti visibilitas log pada teknik *File Analysis* maupun pemblokiran aktif pada *Network Traffic Filtering* dapat terdokumentasi sebagai bukti empiris yang valid. Semua hasil dari tahap-tahap tersebut kemudian dirangkum menjadi satu analisis utama yang menjadi dasar untuk mengambil kesimpulan penelitian.

2.3 Lingkungan Laboratorium Virtual

Eksperimen dilakukan dalam lingkungan laboratorium virtual yang terisolasi sepenuhnya dari jaringan publik guna menjamin keamanan proses simulasi. Infrastruktur ini dibangun menggunakan platform virtualisasi dengan konfigurasi jaringan *Internal Network*. Komponen utama dalam laboratorium ini terdiri dari dua entitas, yaitu mesin penyerang (*Attacker*) menggunakan Kali Linux yang dibekali dengan modul *Adversary Emulation*, dan mesin target (*Victim*) menggunakan Windows 11 Pro sebagai objek implementasi pertahanan. Spesifikasi sistem target dikonfigurasi menyerupai lingkungan kerja standar organisasi guna memastikan relevansi hasil pengujian dengan skenario dunia nyata.



Gambar 2. Topologi Lab Virtual

Gambar 2 di atas merepresentasikan arsitektur dari laboratorium yang digunakan dalam penelitian. Topologi ini berpusat pada sebuah *Virtual Switch* yang berfungsi sebagai media komunikasi tunggal antar-node tanpa akses ke jaringan eksternal. Node Attacker diposisikan sebagai sumber ancaman yang mensimulasikan aktivitas *Command & Control* dan penyebaran *payload*. Sementara itu, Victim 1 dan Victim 2 dikonfigurasi sebagai *endpoint* target di dalam subnet yang sama. Pemilihan struktur dua *victim* ini bertujuan untuk memvalidasi interaksi antar-sistem saat ransomware mencoba melakukan pergerakan lateral (*lateral movement*) di dalam jaringan internal, sehingga efektivitas pemutusan rantai serangan dapat diamati secara komprehensif.

2.4 Desain Kerangka Kerja MITRE D3FEND

Kerangka kerja MITRE D3FEND merupakan ontologi pengetahuan teknik pertahanan siber yang terstruktur dalam enam kategori fungsional utama yaitu *Model, Harden, Detect, Isolate, Deceive,* dan *Evict*. Dalam penelitian ini, desain pertahanan dikonsentrasikan pada tiga kategori utama yang paling relevan untuk mematahkan rantai serangan (*attack chain*) LockBit 3.0 pada level artefak digital.

1) **Harden:**
   Berfokus pada pengurangan celah eksploitasi melalui kebijakan konfigurasi aplikasi dan sistem operasi.
2) **Detect:**
   Menitikberatkan pada visibilitas sistem dalam mengenali aktivitas anomali melalui analisis *file* dan *registry*.

3) **Isolate:**
Bertujuan untuk membatasi ruang gerak ransomware agar tidak terjadi penyebaran lateral melalui jaringan.

Pembatasan pada ketiga kategori ini dilakukan secara sengaja untuk memastikan evaluasi yang mendalam terhadap intervensi artefak digital yang paling krusial, mengingat karakteristik LockBit 3.0 yang sangat bergantung pada manipulasi *registry* dan layanan SMB.

2.5 Skenario Serangan dan Pemetaan Mitigasi

Skenario pengujian disusun berdasarkan dekonstruksi terhadap TTP LockBit 3.0 yang dipetakan secara berhadapan (*head-to-head*) dengan teknik defensif D3FEND. Detail pemetaan teknik serangan dan kontrol mitigasi disajikan dalam Tabel 1 berikut.

Tabel 1. Pemetaan Serangan Ransomware LockBit 3.0

No	Taktik Serangan (ATT&CK)	Kategori D3FEND	Teknik Defensif (D3FEND)	Implementasi Kontrol Teknis
1	Credential Access (T1003.002)	**Detect**	File Analysis (D3-FA)	Mengaktifkan audit akses pada basis data SAM melalui *Registry*.
2	Lateral Movement (T1021.002)	**Isolate**	Network Traffic Filtering (D3-NTF)	Pemblokiran *port* SMB (445) pada sistem target via *Firewall*.
3	Defense Evasion (T1562.001)	**Harden**	Application Config Hardening (D3-ACH)	Penguncian fitur *Tamper Protection* pada antivirus sistem.
4	Impact (T1486)	**Harden**	Local File Access Mediation (D3-LFAM)	Penerapan *Controlled Folder Access* pada folder dokumen.

Penetapan skenario pada Tabel 1 di atas memungkinkan peneliti untuk mengamati interaksi antara *payload* ransomware dengan kebijakan keamanan yang diterapkan secara dinamis. Fokus utama dari desain ini adalah memverifikasi apakah kontrol teknis tersebut mampu menginterupsi jalannya eksekusi *malware* pada titik-titik krusial yang sebelumnya telah dipetakan melalui dekonstruksi TTP. Skenario ini akan diuji secara berulang dalam 50 kali pengujian (*test cases*) untuk memastikan reliabilitas dari setiap teknik mitigasi yang diusulkan terhadap varian LockBit 3.0.

2.6 Kriteria Evaluasi dan Analisis Data

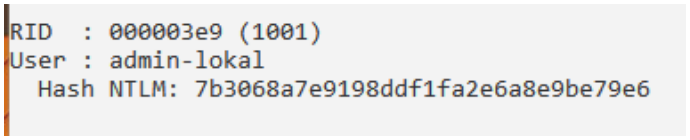
Bagian ini menguraikan parameter yang digunakan untuk menilai efektivitas mitigasi berdasarkan bukti empiris yang dikumpulkan selama eksperimen melalui perbandingan perilaku sistem antara kondisi sebelum (*baseline*) dan sesudah intervensi secara mendalam. Penilaian keberhasilan mitigasi ditetapkan melalui dua kriteria utama, di mana kriteria pertama berfokus pada visibilitas deteksi yang diukur dari kemampuan sistem dalam membangkitkan rekaman log keamanan, seperti Event ID 4663 pada teknik *File Analysis*. Selain itu, kriteria kedua menekankan pada efektivitas pemutusan rantai serangan yang diamati melalui kegagalan teknis penyerang dalam melanjutkan eksekusi ke tahap berikutnya, seperti adanya penolakan koneksi jaringan, kegagalan manipulasi kebijakan keamanan, serta tetap terjaganya integritas file dokumen tanpa adanya perubahan ekstensi oleh proses enkripsi. Seluruh hasil observasi dari kedua fase pengujian tersebut kemudian disandingkan untuk mendapatkan gambaran utuh mengenai kapabilitas kerangka kerja MITRE D3FEND dalam mereduksi dampak serangan LockBit 3.0 secara sistematis.

3. Hasil dan Pembahasan

Bab ini menyajikan temuan teknis dari eksperimen yang dilakukan untuk mengevaluasi kapabilitas MITRE D3FEND terhadap serangan ransomware LockBit 3.0. Pembahasan dibagi menjadi dua bagian utama, yaitu hasil pengujian pada kondisi sistem tanpa proteksi (*baseline*) dan hasil pengujian setelah implementasi kontrol keamanan. Setiap tahapan serangan dan respon sistem didokumentasikan melalui bukti teknis guna memberikan gambaran komprehensif mengenai efektivitas strategi mitigasi yang diterapkan.

3.1 Hasil Pengujian Fase Baseline

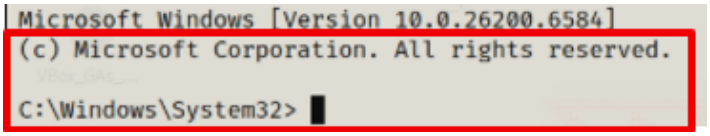
Pengujian baseline dilakukan untuk memetakan tingkat kerentanan sistem standar terhadap rantai serangan LockBit 3.0. Tahapan awal dimulai dengan mensimulasikan taktik *Credential Access* (T1003.002) melalui penggunaan tool Mimikatz guna menguji ketahanan memori sistem terhadap pencurian identitas. Skenario ini dijalankan secara konsisten sebanyak 50 kali iterasi pengujian untuk melihat stabilitas respon memori sistem.



Gambar 3. Keberhasilan Ekstraksi NTLM Hash pada Fase *Baseline*

Gambar 3 di atas menunjukkan keberhasilan serangan Mimikatz dalam mengekstraksi data sensitif dari memori sistem. Dari total 50 kali kasus pengujian yang dilakukan, seluruh percobaan (100%) menunjukkan hasil keberhasilan yang sama. Hasil eksperimen ini membuktikan bahwa tanpa adanya konfigurasi audit registri yang ketat, aktivitas ekstraksi NTLM Hash tersebut dapat berjalan tanpa memicu peringatan apa pun dari sistem keamanan bawaan. Kondisi ini memberikan jalan masuk yang leluasa bagi penyerang untuk menguasai akun administratif sistem secara penuh.

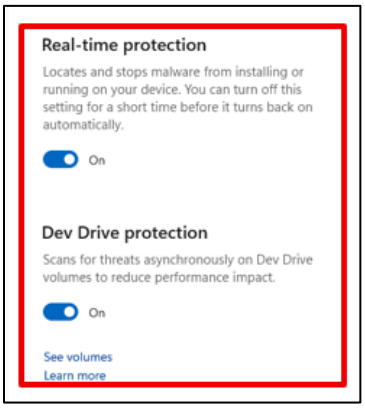
Setelah mendapatkan kredensial yang diperlukan, penyerang melanjutkan serangan dengan taktik *Lateral Movement* (T1021.002) memanfaatkan protokol SMB (*Server Message Block*). Tahap ini bertujuan untuk menyebarkan infeksi dari mesin pertama ke mesin target kedua di dalam satu jaringan yang sama melalui port 445. Sama seperti tahap sebelumnya, pengujian pergerakan lateral ini diulang sebanyak 50 kali iterasi untuk melihat konsistensi keterbukaan jalur komunikasi jaringan.



Gambar 4. Sesi Kendali Jarak Jauh pada Mesin Target Kedua

Gambar 4 memperlihatkan keberhasilan metode *Pass-the-Hash* dalam mendapatkan sesi kendali jarak jauh (*remote command prompt*) melalui port SMB 445. Melalui 50 kali pengujian yang dilakukan, sistem target secara konstan selalu berhasil ditembus dan membuka sesi kendali jarak jauh tanpa ada penolakan dari sistem. Keberhasilan eksploitasi ini mengonfirmasi bahwa keterbukaan jalur komunikasi internal pada konfigurasi standar memberikan ruang bagi ransomware untuk bergerak secara lateral dan mendapatkan hak akses administrator di perangkat lain dalam jaringan organisasi.

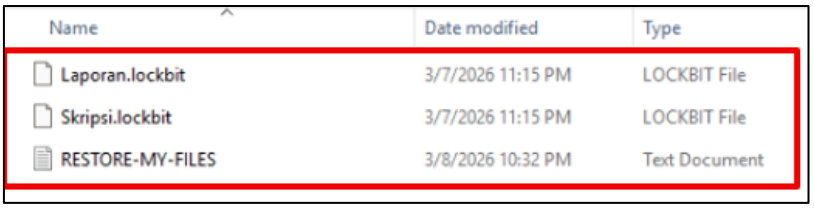
Tahap berikutnya dalam rantai serangan adalah melumpuhkan sistem keamanan lokal melalui serangan *Defense Evasion* (T1562.001). Langkah ini dilakukan dengan menargetkan penonaktifan Windows Defender *Real-time Protection* guna menjamin proses eksekusi payload berbahaya tidak terdeteksi oleh sistem. Iterasi pengujian script pelumpuhan ini juga dieksekusi sebanyak 50 kali kasus terpisah.



Gambar 5. Penonaktifan Fitur Keamanan pada Fase *Baseline*

Berdasarkan Gambar 5, terlihat bahwa serangan melalui baris perintah PowerShell berhasil menonaktifkan fitur *Real-time Protection* secara instan. Dalam 50 kali pengulangan eksperimen, perintah PowerShell tersebut memiliki tingkat keberhasilan mutlak 100% dalam meruntuhkan proteksi lokal. Perubahan status proteksi menjadi OFF tersebut menandakan bahwa mekanisme pertahanan lapis pertama telah runtuh, sehingga sistem berada dalam kondisi sepenuhnya rentan terhadap eksekusi malware lanjutan.

Rangkaian serangan pada fase baseline ini bermuara pada taktik *Impact* (T1486) berupa eksekusi Enkripsi LockBit secara massal. Tahap ini merupakan tujuan akhir dari penyerang untuk menyandera data dan memutus akses pengguna terhadap informasi penting milik mereka. Dampak dari enkripsi filesystem ini diamati secara berulang dalam 50 kali simulasi eksekusi payload.

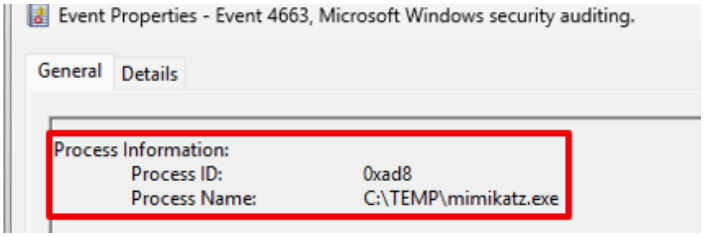


Gambar 6. Kondisi File Target Setelah Enkripsi Massal

Gambar 6 di atas mengilustrasikan hasil akhir dari proses enkripsi yang mengubah seluruh file dokumen menjadi format lockbit. Konsistensi kelumpuhan filesystem ini terbukti dari seluruh 50 iterasi yang dilakukan, di mana tidak ada satu pun file dokumen yang berhasil selamat dari enkripsi massal. Keberhasilan serangan tahap akhir ini menjadi bukti kuat bahwa sistem Windows 11 standar tidak memiliki mekanisme pertahanan aktif yang memadai untuk melindungi filesystem dari modifikasi massal yang dilakukan oleh proses asing secara jarak jauh.

3.2 Hasil Pengujian Fase Mitigasi MITRE D3FEND

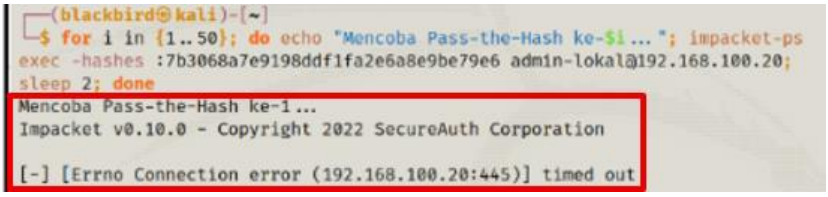
Fase mitigasi dilakukan dengan mengaktifkan teknik pertahanan spesifik untuk menginterupsi jalannya serangan. Pada tahap awal, teknik *File Analysis* (D3-FA) diimplementasikan melalui kebijakan audit registri guna memberikan transparansi terhadap upaya akses ke data sensitif. Skenario pengamanan ini diuji secara konsisten melalui 50 kali pengulangan simulasi serangan menggunakan Mimikatz.



Gambar 7. Deteksi Aktivitas Mencurigakan

Berdasarkan Gambar 7, terlihat bahwa sistem berhasil mendokumentasikan setiap upaya akses ke database SAM secara transparan melalui kemunculan Event ID 4663 pada log keamanan. Dari total 50 kasus pengujian yang dilakukan, sistem secara konstan (100%) berhasil memicu pembentukan log forensik tersebut tanpa ada yang terlewat. Meskipun pada tahap ini sistem pertahanan D3-FA tidak melakukan pemblokiran aktif terhadap jalannya Mimikatz, namun ketersediaan log forensik ini membuktikan bahwa sistem kini memiliki visibilitas penuh terhadap artefak digital yang dimanipulasi oleh penyerang, yang mana pada fase baseline aktivitas ini tidak terdeteksi sama sekali.

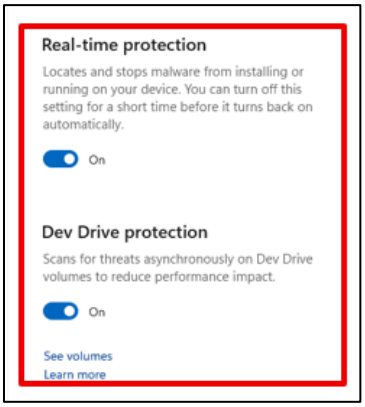
Langkah mitigasi selanjutnya difokuskan pada upaya pembendungan penyebaran di dalam jaringan. Teknik *Network Traffic Filtering* (D3-NTF) diterapkan dengan menutup akses komunikasi yang sering disalahgunakan oleh ransomware untuk bergerak secara lateral. Eksperimen pembendungan pada lapisan jaringan ini dieksekusi kembali sebanyak 50 kali iterasi pengujian.



Gambar 8. Kegagalan Koneksi SMB Akibat Pemblokiran Port 445

Gambar 8 di atas menunjukkan bukti teknis kegagalan serangan pada terminal mesin penyerang yang menghasilkan respon *connection timeout*. Melalui 50 kali kasus pengujian yang dijalankan, seluruh upaya penyerang untuk mengeksploitasi jaringan secara konsisten mengalami kegagalan total. Melalui penguncian port SMB 445 di sisi *firewall* mesin target, setiap upaya koneksi dari penyerang secara konsisten ditolak. Hal ini memvalidasi bahwa rantai penyebaran ransomware telah berhasil diputus pada lapisan jaringan, sehingga infeksi tidak dapat menyebar ke node lain di dalam infrastruktur laboratorium.

Pada lapisan pertahanan aplikasi, pengerasan konfigurasi dilakukan untuk menangkal upaya *Defense Evasion*. Teknik *Application Configuration Hardening* (D3-ACH) digunakan khusus untuk memastikan bahwa agen keamanan sistem tidak dapat dilumpuhkan secara paksa oleh skrip berbahaya. Ketahanan konfigurasi aplikasi ini diuji keandalannya melalui 50 kali iterasi serangan lewat baris perintah.



Gambar 9. Status Proteksi Tetap Aktif Akibat Penerapan D3-ACH

Representasi visual pada Gambar 9 menunjukkan bahwa fitur *Real-time Protection* tetap berada dalam kondisi aktif (ON) dan terkunci meskipun telah menerima instruksi penonaktifan berulang kali melalui PowerShell. Konsistensi ini terbukti dari seluruh 50 percobaan yang dilakukan, di mana tidak ada satu pun instruksi penonaktifan yang berhasil menembus sistem. Melalui aktivasi fitur *Tamper Protection*, perintah penyerang mengalami *silent drop*, di mana instruksi modifikasi tersebut ditolak secara otomatis oleh sistem operasi di latar belakang. Keberhasilan ini memastikan bahwa mekanisme pertahanan lapis pertama tetap terjaga untuk menghadapi fase serangan selanjutnya.

Sebagai benteng terakhir untuk menjaga data pengguna, teknik *Local File Access Mediation* (D3-LFAM) diterapkan. Teknik ini bertujuan untuk melakukan mediasi dan pengawasan ketat terhadap setiap proses yang mencoba melakukan perubahan pada direktori yang berisi informasi krusial. Perlindungan direktori dokumen ini divalidasi keandalannya melalui 50 kali pengulangan eksekusi payload LockBit secara langsung.

Gambar 10. Notifikasi Pemblokiran Modifikasi File oleh D3-LFAM

Berdasarkan Gambar 10, terlihat munculnya notifikasi pemblokiran saat ransomware mencoba melakukan modifikasi atau enkripsi pada file di dalam folder yang dilindungi. Dari 50 kasus simulasi enkripsi yang dilepaskan, fitur keamanan ini sukses 100% menghalau aktivitas ilegal tersebut. Bukti ini menunjukkan bahwa fitur *Controlled Folder Access* berhasil membedakan antara proses sistem yang sah dan proses berbahaya yang mencoba memanipulasi data secara ilegal. Dengan demikian, integritas file tetap terjaga sepenuhnya dan tujuan akhir dari serangan ransomware untuk menyandera data berhasil digagalkan secara total.

3.3 Rekapitulasi dan Analisis Statistik Hasil Eksperimen

Setelah mendokumentasikan proses teknis pada setiap tahapan serangan, bagian ini menyajikan ringkasan data dari total 50 kali iterasi pengujian untuk memverifikasi konsistensi hasil. Perbandingan antara kondisi sistem tanpa proteksi (*baseline*) dan setelah implementasi MITRE D3FEND disajikan pada Tabel 2 berikut.

Tabel 2. Pemetaan Serangan Ransomware LockBit 3.0

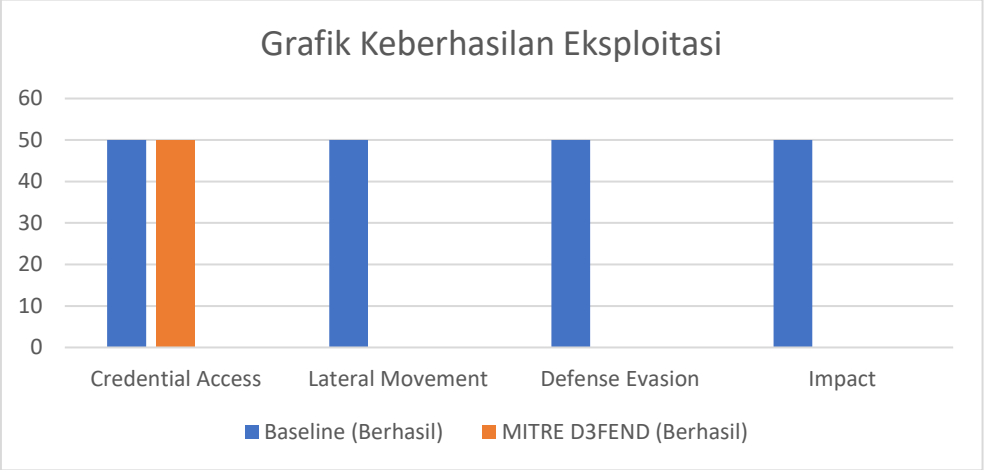
No	Teknik Serangan (ATT&CK)	Baseline (Serangan Berhasil)	MITRE D3FEND (Serangan Berhasil)	Status Mitigasi
1	*Credential Access*	50	50	**Tertembus**
2	*Lateral Movement*	50	0	**Terblokir**
3	*Defense Evasion*	50	0	**Terblokir**
4	*Impact*	50	0	**Terblokir**
	Skor Efektivitas (%)	**0%**	**75%**	

Berdasarkan Tabel 2 di atas, terlihat perbedaan hasil yang sangat kontras antara kondisi baseline dan setelah implementasi MITRE D3FEND. Pada fase *baseline*, seluruh rangkaian serangan LockBit 3.0 sukses seratus persen dengan mencatatkan angka 50 dari 50 keberhasilan percobaan di setiap tahapan, yang membuktikan kerentanan total dari sistem standar. Namun, setelah kontrol MITRE D3FEND diterapkan, terjadi perubahan angka yang signifikan pada setiap teknik serangan dengan pemaknaan yang mendalam.

Pada teknik *Credential Access*, angka keberhasilan serangan tetap berada di nilai 50 dari 50 percobaan karena teknik File Analysis bekerja sebagai deteksi pasif yang sengaja membiarkan Mimikatz berjalan demi merekam 50 log *forensik Event* ID 4663 agar serangan tidak lagi tersembunyi. Sebaliknya, pada teknik *Lateral Movement*, terjadi penurunan angka keberhasilan yang drastis dari 50 menjadi 0 karena teknik *Network Traffic Filtering* melalui

penutupan port SMB 445 memiliki keandalan mutlak dalam memblokir seluruh upaya penyebaran *ransomware* di lapisan jaringan. Penurunan angka dari 50 menjadi 0 juga terjadi pada teknik *Defense Evasion* yang mengonfirmasi bahwa pengerasan konfigurasi aplikasi melalui Tamper Protection sukses melindungi integritas Windows Defender sehingga seluruh skrip PowerShell berbahaya konsisten mengalami kegagalan. Akhirnya, pada teknik Impact, angka keberhasilan enkripsi berhasil ditekan dari 50 menjadi 0 yang menjadi indikator paling krusial bagi keselamatan data karena teknik *Local File Access Mediation* terbukti sukses menghalau seluruh simulasi eksekusi payload LockBit 3.0 dan menjaga file dokumen tetap utuh.

Secara keseluruhan, perubahan angka-angka ini menghasilkan skor efektivitas akumulatif sebesar 75%. Data ini membuktikan bahwa kerangka kerja yang diusulkan sangat efektif dalam memadukan fungsi deteksi dan pencegahan aktif untuk memutus rantai serangan sebelum terjadi kerusakan data yang permanen. Untuk memperjelas perbedaan drastis tersebut, hasil rekapitulasi dipetakan ke dalam grafik perbandingan pada Gambar 3.9.



Gambar 11. Grafik Perbandingan Keberhasilan Eksploitasi

Gambar 11 menunjukkan bahwa pada kondisi *baseline*, LockBit 3.0 memiliki tingkat keberhasilan mutlak di semua tahapan. Sebaliknya, pada kondisi MITRE D3FEND, terjadi penurunan drastis hingga titik nol pada mayoritas tahapan serangan. Skor 75% yang diperoleh D3FEND mencerminkan kemampuan kerangka kerja ini dalam memutus rantai serangan pada fase kritis sebelum enkripsi massal terjadi, sekaligus meningkatkan visibilitas pada fase awal yang sebelumnya tidak terdeteksi.

3.4 Pembahasan

Keberhasilan mitigasi yang ditunjukkan dalam rangkaian eksperimen ini membuktikan bahwa strategi pertahanan berbasis artefak digital memiliki kapabilitas yang signifikan dalam menjawab tantangan serangan *ransomware* modern. Masalah utama yang sering ditemukan adalah sulitnya mendeteksi manuver berbahaya yang menyerupai aktivitas sah di dalam sistem. Melalui implementasi teknik defensif yang proaktif, celah sistem pada fase awal berhasil diatasi secara konsisten. Efektivitas kerangka kerja MITRE D3FEND yang diuji dalam riset ini mencapai skor 75%. Angka ini membuktikan resiliensi yang tinggi karena sistem mampu memblokir secara mutlak tiga dari empat fase kritis serangan, yaitu pada lapisan jaringan melalui teknik *Network Traffic Filtering*, pengerasan aplikasi melalui *Application Configuration Hardening*, dan perlindungan berkas melalui *Local File Access Mediation*. Keberhasilan intervensi pada ketiga lapisan tersebut sejalan dengan temuan Mavire yang menegaskan bahwa strategi pertahanan berlapis sangat efektif dalam mereduksi dampak destruktif ransomware pada endpoint [1].

Meskipun demikian, tingkat efektivitas pertahanan dalam riset ini belum mencapai angka 100% akibat adanya celah pada tahap *Credential Access*. Penyebab utama dari kondisi ini adalah karakteristik fungsional teknik File Analysis yang diimplementasikan berbasis pada metode deteksi pasif, bukan pencegahan aktif. Karakteristik deteksi pasif ini membuat sistem sengaja membiarkan eksekusi Mimikatz berjalan demi mengumpulkan visibilitas artefak log forensik. Fenomena ketidakmampuan kontrol pasif dalam menghentikan eksekusi biner secara langsung ini divalidasi oleh kajian teknis Mohamed, yang menunjukkan bahwa aktor ancaman memang

masih dapat meloloskan eksekusi alat tertentu jika agen keamanan hanya dikonfigurasi untuk melakukan audit log tanpa adanya tindakan pemblokiran proses yang agresif [13]. Untuk mencapai tingkat efektivitas maksimal hingga 100% di masa depan, penelitian ini merekomendasikan integrasi kontrol D3FEND dengan mekanisme mitigasi otomatis yang lebih dinamis. Rekomendasi ini didukung oleh konsep sistem ERAD yang dikembangkan oleh Li dan Madisetti, di mana efektivitas pertahanan dapat dioptimalkan secara mutlak melalui otomatisasi tindakan balasan yang adaptif pada level sistem operasi modern sesaat setelah indikator ancaman terdeteksi oleh kontrol keamanan [8].

Secara lebih luas, temuan dalam riset ini memberikan penguatan nyata bagi perkembangan literatur keamanan siber saat ini. Hasil eksperimen ini berhasil menjembatani celah yang sering muncul antara analisis ofensif dan perancangan arsitektur defensif. Dengan memanfaatkan kestabilan kerangka kerja MITRE D3FEND yang telah mencapai versi resmi 1.0 pada awal 2025, penelitian ini membuktikan bahwa struktur pertahanan yang teratur mampu memberikan respon mesin yang presisi terhadap perilaku lawan [15]. Jika selama ini banyak kajian masih terbatas pada pemodelan konseptual atau analisis pasca insiden yang bersifat pasif, penelitian ini memberikan pembuktian empiris melalui 50 kali iterasi pengujian di laboratorium. Penyatuan antara intelijen taktik serangan dengan langkah mitigasi teknis yang divalidasi dalam riset ini membuktikan bahwa strategi pertahanan proaktif memang memiliki reliabilitas tinggi saat diterapkan secara langsung di lapangan, melampaui batasan wacana teoretis yang selama ini mendominasi literatur.

Selain memberikan validasi teknis, kontribusi utama penelitian ini terletak pada penyediaan standar baru dalam mengevaluasi efektivitas kerangka kerja keamanan secara kuantitatif. Temuan ini selaras dengan upaya akselerasi kebijakan ketahanan siber nasional di Indonesia pada tahun 2025 yang menekankan pada perlindungan ruang siber melalui integrasi teknologi pertahanan yang adaptif [16]. Riset ini menghasilkan sebuah cetak biru arsitektural yang dapat langsung diadopsi oleh praktisi untuk memperkeras keamanan infrastruktur terhadap ancaman r*ansomware* yang terus berevolusi. Secara ilmiah, penggunaan metodologi pengujian berulang dengan jumlah sampel yang besar memberikan standar baru dalam mengevaluasi efektivitas sebuah kerangka kerja keamanan secara kuantitatif. Temuan ini tidak hanya menawarkan solusi praktis di lapangan, tetapi juga menjadi pijakan penting bagi penelitian selanjutnya untuk mengeksplorasi penggunaan kecerdasan buatan (AI) dalam otomatisasi kontrol D3FEND agar sistem pertahanan menjadi lebih adaptif di lingkungan sistem operasi modern [17].

4. Simpulan

Berdasarkan hasil eksperimen dan analisis komparatif yang telah dilakukan, penelitian ini menyimpulkan bahwa implementasi kerangka kerja MITRE D3FEND secara efektif mampu meningkatkan resiliensi sistem operasi Windows 11 dalam menghadapi rantai serangan ransomware LockBit 3.0. Temuan utama menunjukkan perbedaan kontras antara kondisi *baseline* yang sepenuhnya rentan dengan kondisi sistem setelah dimitigasi, di mana sistem mampu memberikan respon teknis yang terukur di setiap tahapan intrusi. Meskipun teknik *File Analysis* (D3-FA) hanya berfungsi sebagai kontrol deteksi pasif yang memberikan visibilitas forensik melalui pembentukan log Event ID 4663, tiga teknik lainnya yaitu *Network Traffic Filtering* (D3-NTF), *Application Configuration Hardening* (D3-ACH), dan *Local File Access Mediation* (D3-LFAM) terbukti berhasil bertindak sebagai kontrol pencegahan aktif yang memutus rantai serangan secara *real-time*. Hal ini membuktikan bahwa strategi pertahanan berlapis (*defense-in-depth*) yang berbasis pada pemetaan artefak digital jauh lebih unggul dalam menjaga integritas data dibandingkan konfigurasi standar organisasi. Sebagai prospek pengembangan ke depan, penelitian ini merekomendasikan adanya integrasi otomatisasi kontrol D3FEND berbasis kecerdasan buatan (AI) dengan sistem manajemen deteksi ancaman yang lebih luas guna menciptakan mekanisme pertahanan yang lebih adaptif terhadap varian *malware* dengan teknik polimorfik yang kompleks pada infrastruktur siber yang bersifat dinamis.

Daftar Referensi

[1] S. Mavire, K. B. Muhwati, N. Kota, and J. A. Awoleye, “Mitigating Ransomware in the Energy and Healthcare Sectors through Layered Defense Strategies,” *International Journal of Scientific and Management Research*, vol. 08, no. 04, pp. 143–166, 2025, doi: 10.37502/ijsmr.2025.8609.

[2] N. Suk-On, N. Thiratitsakun, and K. Chimmanee, “Digital Forensic Analysis of Lockbit Ransomware Attack on Operational Technology,” in *8th International Conference on Information Technology 2024, InCIT 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 624–629. doi: 10.1109/InCIT63192.2024.10810564.
[3] CISA, “#StopRansomware: LockBit 3.0,” 2023. Accessed: Apr. 21, 2026. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
[4] Eliando and A. Budi Warsito, “LockBit Black Ransomware On Reverse Shell: Analysis of Infection Ransomware LockBit Black di Dalam Reverse Shell: Analisis Infeksi,” *Cogito Smart Journal*, vol. 9, no. 2, pp. 228–240, 2023.
[5] R. Kaestria, A. Lukman Djatta, M. Erfan, and E. Faiqotul Himmah, “Penerapan Metodologi Forensik Digital Nist Sp 800-86 Pasca Serangan Ransomware Lockbit 3.0 Implementation of the NIST SP 800-86 Digital Forensic Methodology After the LockBit 3 Ransomware Attack,” *Jurnal Sains Komputer dan Teknologi Informasi e-issn*, vol. 8, no. 1, pp. 55–58, Nov. 2025, doi: https://doi.org/10.33084/jsakti.v8i1.11137.
[6] S. Lee, M. Tsai, and S. W. Shieh, “The Game of Spear and Shield in Next Era of Cybersecurity,” *IEEE Trans. Reliab.*, vol. 73, no. 1, pp. 85–92, Mar. 2024, doi: 10.1109/TR.2023.3342874.
[7] CISA, “Understanding Ransomware Threat Actors: LockBit,” 2023. Accessed: Jan. 07, 2026. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[8] X. Li and V. K. Madisetti, “ERAD: Enhanced Ransomware Attack Defense System for Healthcare Organizations,” *Journal of Software Engineering and Applications*, vol. 17, no. 05, pp. 270–296, 2024, doi: 10.4236/jsea.2024.175016.
[9] C. Lanza, A. Lahmadi, and J. François, “Ransomware Analysis: Knowledge Extraction and Classification for Advanced Cyber Threat Intelligence,” *International Journal of Computer Networks & Communications (IJCNC)*, vol. 16, no. 4, pp. 1–96, 2024, [Online]. Available: http://taylorandfrancis.com
[10] A. F. Syifa and M. Salman, “Cyber Kill Chain Framework Approach to Map Potential Attack Vectors on Windows-based OS,” *International Journal of Electrical, Computer, and Biomedical Engineering*, vol. 3, no. 1, pp. 142–156, May 2025, doi: 10.62146/ijecbe.v3i1.107.
[11] A. Husseis, J. L. Flores, A. Bregar, G. Mazzeo, and L. Coppolino, “Enhancing Cybersecurity Proactive Decision-Making Through Attack Tree Analysis and MITRE Framework,” in *Proceedings - International Carnahan Conference on Security Technology*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICCST59048.2023.10726853.
[12] K. Fida Hasan, S. Member, H. Hossain Shajeeb, C. Abeydeera, B. Turnbull, and M. Warren, “ISADM: An Integrated STRIDE, ATT&CK, and D3FEND Model for Threat Modeling Against Real-world Adversaries,” *IEEE Access*, no. 11, 2023.
[13] N. Mohamed, “Study of bypassing Microsoft Windows Security using the MITRE CALDERA Framework,” *F1000Res.*, vol. 11, no. 344, p. 422, Apr. 2022, doi: 10.12688/f1000research.109148.1.
[14] Í. Oliveira *et al.*, “Boosting D3FEND: Ontological Analysis and Recommendations,” in *Frontiers in Artificial Intelligence and Applications*, IOS Press BV, Dec. 2023, pp. 334–348. doi: 10.3233/FAIA231138.
[15] MITRE, “MITRE D3FEND Knowledge Graph,” MITRE Corporation. Accessed: Jan. 04, 2026. [Online]. Available: https://d3fend.mitre.org/
[16] Seri Mughni Sulubara, Virdyra Tasril, and Nurkhalisah Nurkhalisah, “Legal Protection Against Cybercrime from Ransomware Attacks and Evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia’s Defense,” *Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora*, vol. 2, no. 5, pp. 240–249, Aug. 2025, doi: 10.62383/aliansi.v2i5.1234.
[17] R. Gian Aditya Asbath, R. Putra Anugrah, and A. Setiawan, “Analisis Dampak Ransomware Pada Keamanan Data Perusahaan Dan Strategi Mitigasinya,” *Jurnal Kumpulan Ilmu Komputer Dan Perubahan Digital*, vol. 1, no. 1, pp. 17–23, Jun. 2025.