BAB 2
LANDASAN TEORI

2.1 Penelitian Terdahulu

Penelitian mengenai deteksi *ransomware* telah berkembang dari analisis artefak, pemantauan *filesystem*, analisis dinamis, hingga pendekatan berbasis log dan SIEM. Kharraz et al. menunjukkan bahwa aktivitas file-level seperti enkripsi, perubahan file, dan penghapusan file merupakan indikator penting dalam deteksi *ransomware* [8]. Scaife et al. mengembangkan CryptoDrop untuk mendeteksi *ransomware* berdasarkan indikator aktivitas file yang mencurigakan [9]. Continella et al. mengembangkan ShieldFS untuk memantau aktivitas I/O dan menyediakan mekanisme pemulihan terhadap dampak *ransomware* [16]. Begovic et al. mengelompokkan metode deteksi *crypto-ransomware* ke dalam pemantauan API atau *system call*, pemantauan I/O, dan pemantauan *filesystem* [10].

Penelitian berbasis log dan SIEM menunjukkan bahwa deteksi malware dapat diperkuat melalui pengumpulan serta korelasi log endpoint. Mahmoud et al. menggunakan Elastic Stack dan Sysmon untuk analisis dinamis malware berbasis log endpoint [11]. Amami et al. menunjukkan bahwa Wazuh relevan sebagai solusi SIEM *open-source* karena mendukung pemantauan file, deteksi intrusi berbasis host, dan skalabilitas [13]. Younus dan Alanezi menunjukkan bahwa Wazuh dapat digunakan untuk mendeteksi serangan dan perubahan file melalui integrasi SIEM dan IDS [17]. Dhefanni et al. menunjukkan bahwa integrasi Wazuh dan Telegram dapat digunakan untuk mengirimkan notifikasi otomatis terhadap alert keamanan [14].

2.2 Matriks Perbandingan Penelitian Terdahulu

Perbandingan penelitian terdahulu diperlukan untuk menunjukkan posisi penelitian ini terhadap studi-studi sebelumnya. Matriks perbandingan disusun berdasarkan fokus dan pendekatan, platform atau sumber data, keterbatasan, serta relevansi terhadap penelitian ini. Matriks perbandingan ditunjukkan pada Tabel 2.1.

Tabel 2.1. Matriks Perbandingan Penelitian Terdahulu

Penelitian	**Fokus dan Pendekatan**	**Platform/Sumber Data**	**Keterbatasan**	**Relevansi terhadap Penelitian Ini**
Kharraz et al. [8]	Menganalisis perilaku *ransomware* melalui perubahan file, enkripsi, dan penghapusan file.	Aktivitas *filesystem*.	Belum berfokus pada implementasi SIEM operasional dan pemetaan MITRE ATT&CK.	Menjadi dasar pemilihan indikator perubahan file, enkripsi file, dan penghapusan file.
Scaife et al. [9]	Mengembangkan CryptoDrop untuk deteksi dini berdasarkan indikator aktivitas file mencurigakan.	Aktivitas file pengguna.	Tidak membahas korelasi log terpusat, Wazuh, dan pemetaan MITRE ATT&CK.	Mendukung penggunaan indikator perubahan file sebagai dasar deteksi T1486.
Continella et al. [16]	Mengembangkan ShieldFS untuk deteksi dan pemulihan berbasis aktivitas I/O dan *filesystem*.	I/O dan aktivitas *filesystem*.	Fokus pada mekanisme *filesystem*, bukan integrasi SIEM atau dashboard SOC.	Mendukung pentingnya visibilitas FIM terhadap perubahan file pada endpoint.
Begovic et al. [10]	Menyajikan survei deteksi *crypto-ransomware* berdasarkan API, I/O, *system call*, dan *filesystem*.	API, I/O, *system call*, dan *filesystem*.	Tidak menyediakan implementasi rule SIEM spesifik untuk Wazuh.	Menjadi dasar integrasi FIM, Auditd, Syslog, dan YARA sebagai sumber observasi.
Chew et al. [18]	Mendeteksi perilaku *crypto-ransomware* menggunakan pola *system call*.	Aktivitas sistem operasi.	Tidak berfokus pada integrasi Wazuh, dashboard, dan notifikasi SOC.	Menjadi dasar penggunaan Auditd untuk menangkap aktivitas proses dan perintah.
Lemmou et al. [19]	Menganalisis nama dan isi file *ransom note* sebagai indikator identifikasi *ransomware*.	Nama dan isi file *ransom note*.	Tidak mencakup korelasi multi-sumber log atau validasi SIEM.	Menjadi dasar rule deteksi artefak *ransom note* pada T1486.
Mahmoud et al. [11]	Menggunakan SIEM berbasis Elastic Stack untuk mengumpulkan dan menganalisis perilaku malware.	Log endpoint dan Elastic Stack.	Tidak spesifik pada Wazuh dan skenario *ransomware* Linux.	Menjadi baseline penggunaan SIEM untuk analisis perilaku malware berbasis log.
Amami et al. [13]	Mengevaluasi Wazuh sebagai solusi SIEM *open-source*.	Wazuh.	Tidak spesifik pada validasi rule *ransomware* berbasis MITRE ATT&CK.	Menjadi dasar pemilihan Wazuh sebagai platform utama penelitian.

2.3 Ransomware

Ransomware adalah jenis *malware* yang membatasi akses terhadap data atau sistem dan meminta tebusan kepada korban. Bentuk yang dominan adalah *crypto-ransomware*, yaitu *ransomware* yang mengenkripsi file korban agar tidak dapat diakses tanpa kunci dekripsi [2]. Dalam konteks modern, *ransomware* juga dapat melibatkan pencarian file bernilai, penghapusan cadangan, dan pembuatan *ransom note* [1]. MITRE ATT&CK mengelompokkan aktivitas enkripsi data untuk mengganggu ketersediaan sebagai teknik T1486 *Data Encrypted for Impact* [6].

Dalam penelitian ini, *ransomware* dipahami sebagai rangkaian perilaku yang dapat diamati melalui endpoint. Pemahaman ini sejalan dengan penelitian yang menempatkan aktivitas *filesystem* sebagai sumber informasi penting untuk membedakan perilaku *ransomware* dari aktivitas normal [8].

2.4 Security Information and Event Management (SIEM)

SIEM merupakan platform yang digunakan untuk mengumpulkan, menormalisasi, mengorelasikan, dan menganalisis log keamanan dari berbagai sumber. SIEM relevan untuk penelitian ini karena deteksi *ransomware* membutuhkan korelasi antara aktivitas file, aktivitas proses, log sistem, dan hasil pemindaian artefak [11]. Dalam konteks operasional keamanan, SIEM membantu analis menelusuri rangkaian kejadian dari log mentah menjadi alert yang memiliki konteks investigasi.

2.5 Wazuh

Wazuh merupakan platform keamanan *open-source* yang menyediakan fungsi SIEM dan HIDS. Wazuh mendukung pemantauan file, korelasi rule, integrasi log endpoint, serta visualisasi alert untuk mendukung analisis keamanan [13]. Dokumentasi Wazuh menjelaskan bahwa platform ini menyediakan kemampuan SIEM dan XDR untuk pengumpulan serta analisis data keamanan [12].

2.6 File Integrity Monitoring (FIM)

FIM digunakan untuk memantau perubahan file, seperti pembuatan, modifikasi, penghapusan, dan perubahan metadata file. Dalam penelitian ini, FIM digunakan untuk mendeteksi pembuatan file berekstensi *ransomware*, pembuatan

ransom note, dan penghapusan file pada direktori uji. FIM relevan karena banyak indikator *ransomware* dapat diamati melalui perubahan struktur dan nama file pada endpoint [20].

2.7 Auditd

Auditd digunakan untuk merekam aktivitas pada tingkat sistem operasi Linux, termasuk eksekusi perintah dan *system call*. Dalam penelitian ini, Auditd digunakan untuk menangkap aktivitas *file discovery*, perubahan izin file, penghapusan file, transfer alat, dan penghambatan mekanisme pemulihan. Integrasi Auditd dengan Wazuh digunakan agar log Linux Audit dapat diproses menjadi event dan alert pada Wazuh [21]. Chew et al. menunjukkan bahwa pola *system call* dapat digunakan untuk mendeteksi perilaku *ransomware* secara real time [18].

2.8 YARA

YARA digunakan untuk mengidentifikasi file berdasarkan pola string atau struktur tertentu. Dokumentasi YARA menjelaskan bahwa YARA membantu peneliti malware mengidentifikasi dan mengklasifikasikan sampel berdasarkan pola tekstual atau biner [22]. Dalam penelitian ini, YARA digunakan untuk mendeteksi artefak yang merepresentasikan pola enkripsi dan *ransom note* tanpa menjalankan *ransomware* aktif. Pada Wazuh, hasil pemindaian YARA dapat digunakan sebagai event yang diproses oleh decoder dan rule untuk menghasilkan alert [23].

2.9 MITRE ATT&CK

MITRE ATT&CK adalah basis pengetahuan yang mendokumentasikan taktik dan teknik adversary berdasarkan observasi serangan nyata. Dalam penelitian ini, MITRE ATT&CK digunakan untuk memetakan setiap rule ke teknik yang relevan agar alert memiliki konteks analisis yang jelas [15].

Teknik T1486 menjelaskan aktivitas enkripsi data untuk mengganggu ketersediaan data atau sistem korban [6]. Teknik T1490 menjelaskan upaya adversary untuk menonaktifkan atau menghapus fitur pemulihan sistem agar dampak serangan lebih sulit dipulihkan [7]. Teknik T1083 menjelaskan aktivitas enumerasi file dan direktori menggunakan utilitas seperti `find`, `ls`, atau `locate` [24]. Teknik T1222 menjelaskan perubahan izin atau atribut file dan direktori yang

dapat memengaruhi kontrol akses [25]. Teknik T1059 menjelaskan penyalahgunaan interpreter perintah atau skrip untuk menjalankan perintah, skrip, atau binary [26]. Teknik T1070.004 menjelaskan penghapusan file sebagai bagian dari pengurangan jejak aktivitas [27]. Teknik T1105 menjelaskan transfer alat atau file ke lingkungan korban [28].

2.10 Dasar Pemilihan Sembilan Rule Utama

Pemilihan sembilan rule utama dilakukan berdasarkan relevansi teknik terhadap perilaku *ransomware*, ketersediaan telemetri pada endpoint Linux, dan kemampuan rule untuk divalidasi secara aman tanpa menjalankan malware aktif. Ringkasan dasar pemilihan rule disajikan pada Tabel 2.2.

Tabel 2.2. Dasar Pemilihan Sembilan Rule Utama

No	**Rule**	**MITRE**	**Sumber Deteksi**	**Dasar Ilmiah**
1	Ekstensi *ransomware*	T1486	FIM	T1486 menjelaskan enkripsi data untuk mengganggu ketersediaan, termasuk perubahan file yang membuat data tidak dapat diakses [6].
2	*Ransom note*	T1486	FIM/YARA	Nama dan isi *ransom note* dapat digunakan sebagai indikator identifikasi *ransomware* [19].
3	Pola enkripsi YARA	T1486	YARA	YARA mendukung identifikasi artefak berdasarkan pola tekstual atau biner pada file yang dipindai [22].
4	*Inhibit recovery*	T1490	Auditd/YARA	T1490 menjelaskan upaya menghapus atau menonaktifkan fitur pemulihan agar dampak serangan lebih sulit dipulihkan [7].

No	Rule	MITRE	Sumber Deteksi	Dasar Ilmiah
5	*File discovery*	T1083	Auditd	T1083 menjelaskan aktivitas enumerasi file dan direktori menggunakan utilitas sistem seperti `find` atau `ls` [24].
6	*Permission modification*	T1222	Auditd	T1222 menjelaskan perubahan izin atau atribut file dan direktori untuk memengaruhi kontrol akses [25].
7	*Script execution*	T1059	Syslog/Auditd	T1059 menjelaskan penyalahgunaan interpreter perintah atau skrip untuk menjalankan perintah, skrip, atau binary [26].
8	*File deletion*	T1070.004	Auditd/FIM	T1070.004 menjelaskan penghapusan file untuk mengurangi jejak aktivitas atau menghapus artefak tertentu [27].
9	*Ingress tool transfer*	T1105	Auditd	T1105 menjelaskan transfer alat atau file ke lingkungan korban sebagai bagian dari operasi adversarial [28].