BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Ancaman siber terus berkembang dan menjadi tantangan penting bagi organisasi karena dapat mengganggu operasional, menurunkan ketersediaan layanan, dan menimbulkan kerugian finansial. CISA menempatkan *ransomware* sebagai ancaman yang perlu ditangani melalui langkah pencegahan, deteksi, respons, dan pemulihan yang terstruktur [1]. *Ransomware* adalah jenis *malware* yang membatasi akses korban terhadap data atau sistem dan meminta tebusan agar akses tersebut dipulihkan [2].

Urgensi penelitian ini diperkuat oleh realitas ancaman siber terkini yang menempatkan *ransomware* sebagai salah satu vektor serangan paling merugikan secara finansial maupun operasional. Laporan *Cost of a Data Breach* mencatat bahwa rata-rata biaya pelanggaran data global terus meningkat hingga mencapai angka tertinggi, dan insiden yang terungkap melalui pemerasan *ransomware* membebani organisasi dengan biaya yang lebih tinggi dibandingkan rata-rata insiden lainnya [3]. ENISA juga menempatkan *ransomware* sebagai salah satu ancaman paling dominan dalam lanskap ancaman siber [4]. Selain dimensi biaya, faktor kecepatan deteksi terbukti menjadi penentu besarnya kerugian, sehingga kemampuan deteksi dini berbasis perilaku menjadi jauh lebih bernilai daripada respons setelah proses enkripsi terjadi [3]. Pada saat yang sama, *ransomware* modern semakin sulit dikenali oleh pendekatan berbasis *signature* karena memanfaatkan teknik *polymorphism*, *obfuscation*, dan eksekusi *fileless* yang mampu menghasilkan varian baru lebih cepat daripada pembaruan basis *signature* [5]. Kondisi tersebut menjadikan integrasi SIEM berbasis Wazuh yang dipadukan dengan kerangka MITRE ATT&CK relevan dan krusial, karena memungkinkan organisasi membangun visibilitas perilaku *ransomware* secara terstruktur, terukur, dan dapat ditelusuri, termasuk bagi organisasi dengan keterbatasan anggaran keamanan [1].

Serangan *ransomware* modern tidak dapat dipahami hanya sebagai proses enkripsi file, karena serangan tersebut mencakup tahapan pencarian file, eksekusi perintah, perubahan atribut file, penghapusan artefak, transfer alat, dan penghambatan mekanisme pemulihan. MITRE ATT&CK memetakan enkripsi data

sebagai teknik T1486 *Data Encrypted for Impact* [6] dan penghambatan pemulihan sebagai teknik T1490 *Inhibit System Recovery* [7]. Kharraz et al. menunjukkan bahwa aktivitas pada tingkat *filesystem* merupakan karakteristik penting dalam memahami perilaku *ransomware* [8].

Pendekatan deteksi berbasis *signature* memiliki keterbatasan ketika berhadapan dengan varian baru atau pola serangan yang berubah. Scaife et al. menunjukkan bahwa deteksi dini *ransomware* dapat dilakukan melalui indikator perilaku file yang mencurigakan, sehingga analisis perilaku menjadi pendekatan yang relevan untuk mengurangi dampak enkripsi [9]. Begovic et al. mengelompokkan pendekatan deteksi *crypto-ransomware* ke dalam tiga kelompok utama, yaitu pemantauan API atau *system call*, pemantauan I/O, dan pemantauan aktivitas *filesystem* [10].

Dalam konteks operasional keamanan, *Security Information and Event Management* (SIEM) digunakan untuk mengumpulkan, menormalisasi, mengorelasikan, dan menganalisis data log dari berbagai sumber. Mahmoud et al. menunjukkan bahwa integrasi SIEM dengan log endpoint dan MITRE ATT&CK dapat membantu analisis perilaku malware secara lebih terstruktur [11]. Wazuh menyediakan kemampuan SIEM dan HIDS yang mendukung pengumpulan log endpoint, FIM, integrasi Auditd, integrasi YARA, *custom rules*, visualisasi alert, dan integrasi notifikasi [12, 13, 14]. Framework MITRE ATT&CK dirancang sebagai basis pengetahuan taktik dan teknik adversary berdasarkan observasi serangan nyata sehingga alert yang dihasilkan tidak hanya dipahami sebagai peringatan teknis [15].

Berdasarkan latar belakang tersebut, penelitian ini mengusulkan integrasi SIEM berbasis Wazuh untuk mendeteksi indikator perilaku *ransomware* pada endpoint Linux, dengan fokus validasi pada sembilan rule utama yang merepresentasikan teknik T1486, T1490, T1083, T1222, T1059, T1070.004, dan T1105 dalam MITRE ATT&CK.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah penelitian ini adalah sebagai berikut.

1. Bagaimana perilaku *ransomware* pada infrastruktur TI dapat diidentifikasi melalui aktivitas *endpoint* dan log sistem?

2. Bagaimana sistem deteksi berbasis Wazuh dan MITRE ATT&CK dapat dibangun dan divalidasi secara fungsional untuk mendeteksi, memetakan, dan mengirimkan notifikasi serangan *ransomware*?

1.3 Batasan Permasalahan

Agar ruang lingkup penelitian tetap terarah, batasan penelitian ini adalah sebagai berikut.

1. Pengujian menggunakan simulasi perilaku yang aman dan terkendali, bukan eksekusi *ransomware* aktif.
2. Validasi difokuskan pada sembilan rule utama, yaitu T1486 ekstensi *ransomware*, T1486 *ransom note*, T1486 pola enkripsi YARA, T1490 *inhibit recovery*, T1083 *file discovery*, T1222 *permission modification*, T1059 *script execution*, T1070.004 *file deletion*, dan T1105 *ingress tool transfer*.
3. Penelitian tidak mengukur performa deteksi secara general pada dataset besar atau lingkungan produksi. Metrik evaluasi hanya digunakan sebagai evaluasi terbatas berdasarkan skenario laboratorium.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut.

1. Mengidentifikasi perilaku *ransomware* pada infrastruktur TI melalui aktivitas *endpoint* dan log sistem.
2. Membangun dan memvalidasi sistem deteksi berbasis Wazuh dan MITRE ATT&CK yang mampu mendeteksi, memetakan, dan mengirimkan notifikasi serangan *ransomware* secara fungsional.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut.

1. Memberikan rancangan implementatif mengenai integrasi Wazuh, FIM, Auditd, Syslog, YARA, dan MITRE ATT&CK untuk deteksi perilaku *ransomware*.

2. Menjadi referensi teknis bagi analis keamanan dalam membangun mekanisme deteksi berbasis SIEM yang dapat diuji secara fungsional.

3. Memberikan contoh matriks validasi fungsional yang menghubungkan aktivitas simulasi, sumber log, rule Wazuh, alert, notifikasi, skor indikasi, metrik evaluasi, dan teknik MITRE ATT&CK.

1.6 Sistematika Penulisan

Sistematika penulisan laporan penelitian ini adalah sebagai berikut.

- **Bab 1 Pendahuluan** menjelaskan latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan.
- **Bab 2 Landasan Teori** membahas penelitian terdahulu, *ransomware*, SIEM, Wazuh, FIM, Auditd, YARA, MITRE ATT&CK, dan dasar pemilihan sembilan rule utama.
- **Bab 3 Metodologi Penelitian** menjelaskan metode eksperimen laboratorium, alur penelitian, arsitektur sistem tiga lapis beserta alur perancangan sistem dari *endpoint* hingga notifikasi, konfigurasi komponen, desain rule, skenario simulasi, skenario aktivitas normal, dan metode validasi fungsional.
- **Bab 4 Hasil dan Pembahasan** menyajikan hasil implementasi, hasil pengujian sembilan skenario, rekapitulasi validasi fungsional, skor indikasi, evaluasi dan penyempurnaan rule deteksi, simulasi ketahanan terhadap 50 aktivitas *legitimate*, serta pembahasan performa dan keterbatasan deteksi.
- **Bab 5 Simpulan dan Saran** memuat simpulan berdasarkan hasil validasi dan saran pengembangan penelitian.