BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan transformasi digital mendorong meningkatnya ketergantungan organisasi terhadap sistem informasi, sehingga keamanan siber menjadi aspek yang semakin krusial. Secara global, ancaman siber terus mengalami peningkatan baik dari segi kuantitas maupun kecanggihan serangan. Di Indonesia, tren serangan siber juga menunjukkan eskalasi yang signifikan, di mana serangan sering kali menyasar celah keamanan pada sistem yang tidak tertangani dengan baik (Security *et al.,* 2022)**.** Nurhidayat *et al.* (2024), menegaskan bahwa kerentanan sistem elektronik merupakan risiko utama yang harus dikelola secara proaktif. Tanpa manajemen kerentanan yang baik, organisasi berisiko mengalami eksploitasi yang dapat mengganggu keberlangsungan operasional. Oleh karena itu, organisasi perlu memiliki mekanisme prioritisasi kerentanan yang akurat dan berbasis data.

Penilaian risiko kerentanan pada beberapa organisasi masih bergantung pada *CVSS Base Score* sebagai indikator utama. Namun, pendekatan ini memiliki keterbatasan karena skor dasar seringkali gagal mencerminkan risiko aktual di lingkungan operasional yang spesifik. Dokumen standar manajemen kerentanan nasional menyebutkan bahwa penilaian risiko harus melampaui skor teknis semata dengan mempertimbangkan validasi dan konteks lingkungan organisasi (Nurhidayat *et al.,* 2024). Hal ini didukung oleh penelitian Walkowski *et al.* (2021), yang membuktikan bahwa penggunaan skor dasar saja tidak akurat karena mengabaikan parameter lingkungan (*Environmental Score*). Kerentanan dengan skor rendah dapat berubah menjadi risiko kritis jika berada pada aset yang vital. Hal ini menunjukkan bahwa pendekatan penilaian berbasis satu kriteria belum memadai untuk menentukan urgensi penanganan kerentanan.

Tantangan tersebut semakin kompleks ketika organisasi harus menangani banyak kerentanan secara bersamaan dengan keterbatasan sumber daya. Nurhidayat *et al.* (2024), merekomendasikan agar penanganan kerentanan diprioritaskan berdasarkan tingkat

kritikalitas aset dan ketersediaan sumber daya perbaikan. Sejalan dengan itu, faktor-faktor kontekstual seperti usia kerentanan (*Age in Days*), jumlah perangkat terdampak (*Device Count*), serta ketersediaan pembaruan keamanan (*Update Availability*) menjadi variabel kunci dalam menentukan prioritas remediasi yang efektif (Kodrat, 2024; Walkowski *et al.,* 2021).

Pendekatan *Multi-Criteria Decision Making* (MCDM), khususnya metode *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS), menyediakan kerangka yang sistematis untuk mengevaluasi alternatif berdasarkan banyak kriteria. Studi terbaru dari (Zulfa *et al.,* 2025), membuktikan bahwa metode TOPSIS efektif diimplementasikan dalam sistem informasi berbasis web untuk menentukan prioritas penanganan pengaduan secara objektif berdasarkan kriteria urgensi dan dampak. Selain itu, penggunaan TOPSIS dalam sistem pendukung keputusan juga terbukti mampu menghasilkan rekomendasi peringkat yang mendekati kondisi ideal berdasarkan preferensi yang ditentukan (Darmawan *et al.,* 2021; Pohan *et al.,* 2025). Efektivitas ini menjadikan TOPSIS metode yang tepat untuk diterapkan dalam manajemen kerentanan siber yang melibatkan ketidakpastian data dan kriteria yang beragam (Alnajim *et al.,* 2026).

Berdasarkan kebutuhan tersebut, penelitian ini menerapkan metode TOPSIS untuk menentukan urutan prioritas penanganan kerentanan perangkat lunak menggunakan empat kriteria utama yaitu *Severity Score, Device Count, Age in Days, dan Update Score*. Pendekatan ini diharapkan menghasilkan pemeringkatan kerentanan yang lebih akurat berdasarkan data operasional *Kaspersky Security Center* yang digunakan PT PLN Nusa Daya. Hasil penelitian ini diharapkan menjadi dasar pendukung keputusan dalam proses manajemen *patch* serta membantu perusahaan memfokuskan upaya remediasi pada kerentanan yang memiliki risiko tertinggi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka permasalahan dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana menerapkan metode TOPSIS untuk menentukan prioritas penanganan kerentanan perangkat lunak berdasarkan kriteria *Severity Score, Device Count, Age in Days,* dan *Update Score?*
2. Bagaimana hasil pemeringkatan kerentanan yang diperoleh setelah metode TOPSIS diterapkan pada dataset kerentanan *Kaspersky Security Center*?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini adalah untuk:

1. Menerapkan metode TOPSIS untuk menentukan prioritas penanganan kerentanan perangkat lunak berdasarkan kriteria *Severity Score, Device Count, Age in Days,* dan *Update Score.*
2. Menghasilkan pemeringkatan kerentanan perangkat lunak berdasarkan nilai preferensi (C_i) yang diperoleh dari proses perhitungan TOPSIS.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Manfaat Teoritis

Penelitian ini memberikan kontribusi pada kajian keamanan informasi dan pengambilan keputusan multikriteria (MCDM) melalui penerapan metode TOPSIS untuk penentuan prioritas kerentanan perangkat lunak. Integrasi variabel *Severity Score, Device Count, Age in Days, dan Update Score* memperkuat pendekatan kuantitatif dalam analisis risiko keamanan berbasis data operasional.

2. Manfaat Praktis
    1) Memberikan hasil pemeringkatan kerentanan yang dapat dimanfaatkan PT PLN Nusa Daya untuk memfokuskan upaya remediasi pada kerentanan yang memiliki tingkat risiko paling tinggi.
    2) Mendukung proses pengambilan keputusan berbasis data dalam manajemen kerentanan dan *patch management*, sehingga membantu perusahaan meningkatkan efisiensi, mengurangi risiko eksploitasi, serta memperkuat ketahanan keamanan sistem informasi.

1.5 Ruang Lingkup Masalah

Adapun batasan yang digunakan dalam penelitian ini dijabarkan sebagai berikut.

1. Data kerentanan yang dianalisis berasal dari hasil pemindaian *Kaspersky Security Center* pada periode Juni hingga Agustus 2025 dan dibatasi hanya pada rentang waktu tersebut.
2. Data yang dianalisis merupakan data kerentanan perangkat lunak aktif hasil monitoring keamanan siber di lingkungan PT PLN Nusa Daya.
3. Penelitian ini hanya menggunakan empat variabel utama yang tersedia dalam dataset, yaitu *Severity Score* (skala 1–4), *Device Count* (jumlah perangkat terdampak), *Age in Days* (usia kerentanan dalam satuan hari), dan *Updates Score* (ketersediaan pembaruan dengan nilai 0 atau 1). Variabel lain di luar keempat kriteria tersebut tidak dimasukkan ke dalam proses analisis.
4. Metode yang digunakan adalah *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS) untuk pemeringkatan prioritas kerentanan. Metode MCDM lain tidak dibahas maupun dibandingkan.

1.6 Kebaharuan

Kebaruan dalam penelitian ini ditekankan pada pendekatan yang digunakan dalam proses prioritisasi kerentanan, baik dari sisi sumber data, penetapan kriteria, maupun validasi hasil analisis. Adapun kebaruan penelitian ini meliputi:

1. Penerapan metode TOPSIS menggunakan data kerentanan operasional aktual dari *Kaspersky Security Center* PT PLN Nusa Daya, bukan dataset publik.
2. Penetapan kriteria *Severity Score, Update Score, Age in Days, dan Device Count* berdasarkan kajian literatur dan *expert judgment* internal sehingga sesuai konteks operasional.
3. Verifikasi hasil melalui perbandingan perhitungan manual TOPSIS dan implementasi berbasis Python untuk menjamin akurasi analisis.