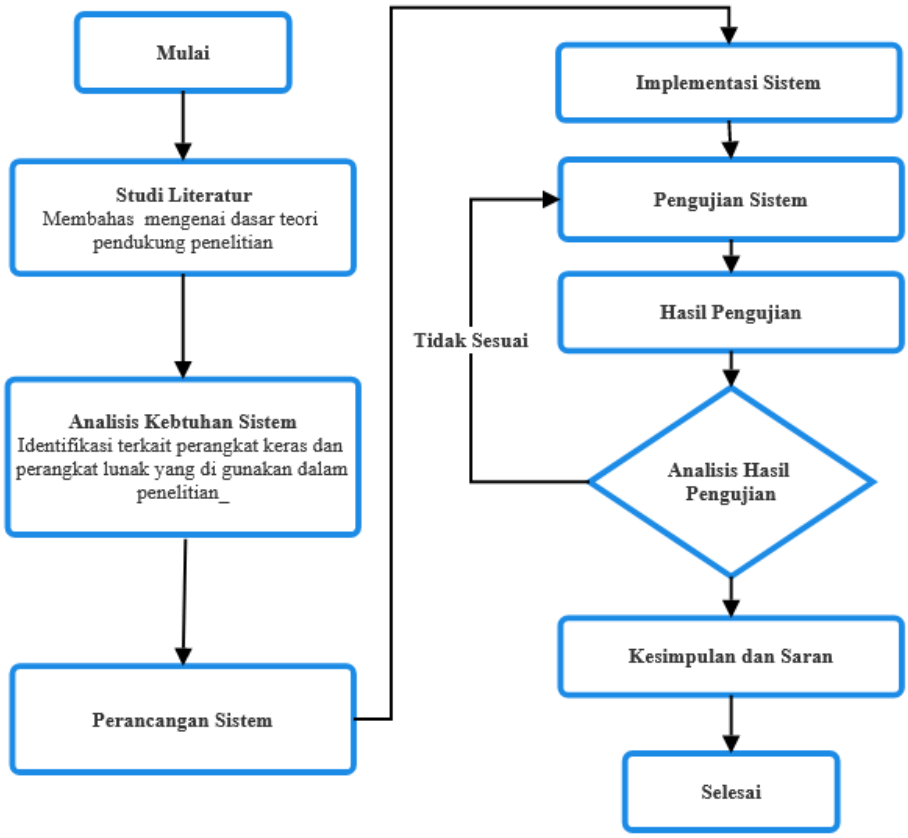
BAB III

METODOLOGI PENELITIAN

3.1 Tahapan Penelitian



Gambar 3. 1 Diagram Alur Penelitian

Tahapan Penelitian ini secara keseluruhan disajikan menggunakan diagram alur penelitian. Diagram alur penelitian ini dapat di lihat pada gambar 3.1. Diagram alur penelitian merupakan prosedur untuk melakukan penelitian yang dimulai dari tahap studi literatur tahap analisis kebutuhan sistem, tahap perancangan, tahap implemetasi, dan tahap analisis hasil pengujian.

Studi literatur merupakan tahapan untuk memenuhi kebutuhan data, melakukan eksplorasi konsep dan teori yang berkaitan dengan *SIEM*, log analisis dan *CTI*. Studi literatur yang dilakukan diperoleh dari berbagai sumber diantaranya yaitu jurnal, e-book, artikel dan lain sebagainya. Kajian studi literatur menggunakan aplikasi *Harzing's Publish or Perish*. Indikator keberhasilan dari tahapan ini adalah memahami domain penelitan, mengdentifikasi peluang penelitian serta menetapkan tujuan dan pertanyaan penelitian, luaran dari tahapan ini adalah Bab I pendahuluan dan Bab II tinjauan Pustaka.

3.2 Analisis Kebutuhan Sistem

Analisis Kebutuhan sistem bertujuan untuk mengetahui elemen apa saja yang di butuhkan dalam melaksanakan penelitian ini untuk mendapatkan gambaran umum sistem. Kebutuhan sistem yang digunakan dalam penelitian ini terbagi menjadi dua jenis, yaitu kebutuhan *Software* dan *Hardware:*

Tabel 3. 1 Kebutuhan Hardware

Requirement	Hardware yang di gunakan
2 core Processor	Processor Intel Core I3-5005U
8 GB Ram	12 GB Ram
50 GB storage	128 GB SSD

Tabel 3.1 merupakan kebutuhan perangkat keras yang dibutuhkan oleh sistem, dan juga hardware yang akan di gunakan pada penelitian. Sistem yang akan di bangun memiliki *requirement minimum* menggunakan *Processor 2 core, 8GB memory,* dan penyimpanan minimal 50 GB. Sistem yang di gunakana memiliki

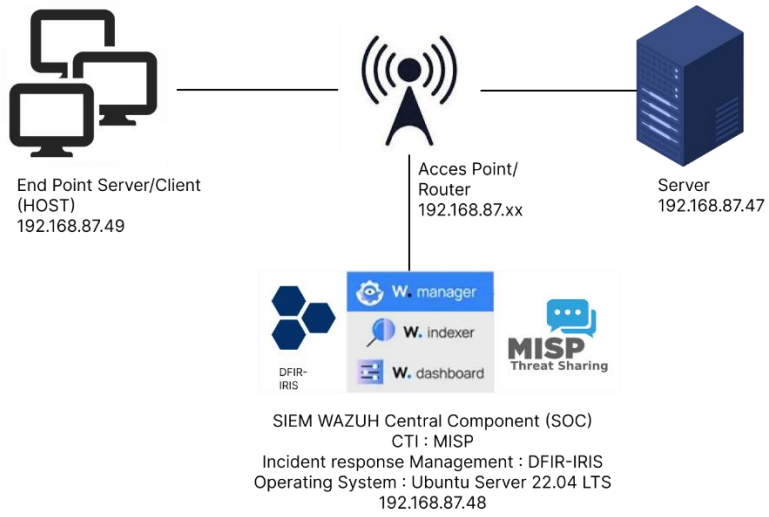
spesifikasi *processor Intel Core I3-5005U 2 core*, 12 GB *Memory*, dan pentimpanan sebesar 120 GB SSD.

Tabel 3. 2 Kebutuhan Software

Operating System	Microsoft Windows 10 Pro, Linux: Ubuntu Server LTS (22.04),
Security Monitoring	*WAZUH* 4.9
Incident Response Mangement	DFIR IRIS
Threat Intelligence	*MISP* – Malware Information Sharing Platform

Tabel 3.2 merupakan kebutuhan perangkat lunak yang dibutuhkan oleh sistem, perangkat lunak apa saja yang akan di gunakan pada penelitian ini. Tabel ini mencakup empat kategori utama, yaitu *Operating System* yang mencakup *Windows 11 Pro* dan *Linux Ubuntu 22.04LTS*, *Security Monitoring* menggunakan *Wazuh 4.9x*, *Log Analytics* dan *incident response manager* dengan *DFIR-IRIS 2.4.3*, dan *Threat Intelligen*ce menggunakan platform berbagi informasi *malware* (*MISP*).

3.3 Perancangan Sistem



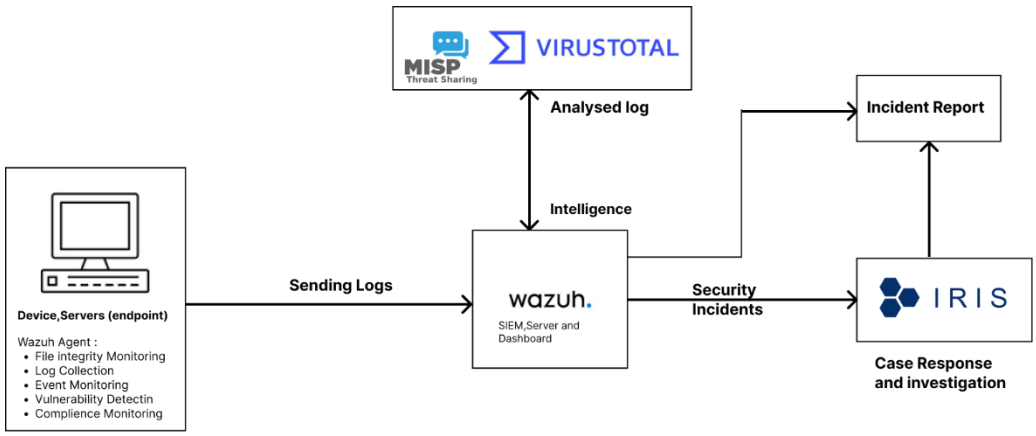
Gambar 3. 2 Topologi Sistem

Perancangan sistem dilakukan untuk membuat desain perencanaan arsitektur sistem yang akan dibangun dapat berjalan sesuai dengan tujuan penelitian. Gambar 3.2 Rencana topologi sistem yang akan dibangun merupakan lingkungan *server* yang menggunakan protokol komunikasi berbasis model *OSI (Open Systems Interconnection)*. *Server* terkoneksi dengan internet melalui sebuah akses point yang mengambil jaringan dari port *WLAN 1*, yang berada *pada layer Physical* dan *Data Link OSI* untuk pengiriman data fisik dan pengaturan pengalamatan MAC. *Port ethernet 1* terhubung dengan *server SIEM* yang memiliki alamat *IP 192.168.87.48*, menggunakan sistem operasi Ubuntu Server versi *22.04 LTS*. *Server SIEM* tersebut dibangun menggunakan *SIEM Wazuh* dan diintegrasikan dengan program *CTI* menggunakan *MISP* pada *layer Application* untuk berbagi informasi ancaman, dan *DFIR IRIS* untuk manajemen respons insiden. *Port ethernet 2* terhubung dengan sebuah *server* menggunakan sistem operasi *ubuntu server 22.04*,

yang juga terhubung ke *access point* melalui alamat IP *192.168.87.47* pada *layer Network OSI* untuk pengalamatan dan *routing data*. *Port ethernet 3* terhubung dengan sebuah *host* atau endpoint menggunakan sistem operasi *Microsoft Windows 11 pro,* yang juga terhubung ke *access point* melalui alamat IP *192.168.87.49* pada *layer Network OSI* untuk pengalamatan dan *routing data*. *Wazuh agent* yang diinstal pada *endpoint* tersebut berfungsi mengirimkan *log system event* ke *server SIEM* melalui protokol pada layer *Transport OSI* untuk memastikan reliabilitas pengiriman data.

3.4 Implemetasi Sistem

Implementasi sistem merupakan proses penelitan, pada tahap ini hasil perancangan sistem di implementasikan sesuai dengan desain yang telah dibuat. Instalasi dan konfigurasi dilakukan sesuai referensi dokumentasi dari masing-masing software yang digunakan.



Gambar 3. 3 Gambaran Cara Kerja Sistem

Gambar 3.3 merupakan Alur kerja sistem tersebut menggambarkan integrasi *SIEM Wazuh* dengan berbagai komponen untuk deteksi dan respons

ancaman siber. *Endpoint* atau *server* dilengkapi dengan *Wazuh Agent* untuk mengumpulkan log, memantau integritas file, mendeteksi kerentanan, dan memantau kepatuhan. Data yang dikumpulkan dikirimkan ke *Wazuh SIEM Server* untuk dianalisis dan dikelola secara terpusat melalui *dashboard*. *Wazuh* terintegrasi dengan platform intelijen ancaman seperti *MISP* untuk berbagi informasi ancaman terkini dan *VirusTotal* untuk memverifikasi *file* atau *URL* mencurigakan. Data yang telah dianalisis kemudian diteruskan ke *DFIR-IRIS* untuk mendukung investigasi forensik dan respons insiden, menghasilkan laporan insiden yang membantu tim keamanan dalam mengambil tindakan lebih lanjut. Integrasi ini memungkinkan deteksi ancaman yang lebih akurat dan respons insiden yang lebih cepat.gambaran sistem yang akan di implentasikan. Sistem yang dibuat menggunakan *OS ubuntu desktop 22.04* sebagai sistem operasinya, *Wazuh* sebagai *SIEM*, *DFIR-IRIS* sebagai *incident response* dan *MISP* sebagai *cyber threat intelligence sharing platform*. Ketiga aplikasi tersebut di integrasikan sehingga membuat sistem *threat hunting incident response*.

3.5 Pengujian Sistem

Pengujian sistem merupakan proses lanjutan dari implementasi sistem yang kemudian akan diuji sesuai skenario pengujian yang telah ditentukan. Pengujian yang akan dilakukan yaitu membandingkan *SIEM Wazuh* Standar dan *SIEM Wazuh* yang telah di integrasikan dengan *MISP* dan *DFIR-Iris*.

Tahapan pengujian dalam penelitian ini melibatkan beberapa skenario untuk menilai efektivitas deteksi *malware* melalui integrasi berbagai komponen. Pengujian akan menggunakan sampel *malware* dari repositori

github.com/ThatSINEWAVE, yang dideploy pada host untuk memicu deteksi. Tiga skema akan diuji secara bertahap, yaitu deteksi *malware* oleh *Wazuh* secara mandiri, integrasi *Wazuh* dengan *MISP*, dan integrasi *Wazuh* dengan *MISP* serta *DFIR-IRIS* untuk *incident response*. Setiap skema ini akan dievaluasi berdasarkan beberapa metrik, yaitu *True Positive (TP), False Positive (FP), False Negative (FN), dan True Negative (TN)*.

3.6 Analisis Hasil Pengujian

Berdasarkan hasil pengujian maka dilakukan evaluasi menggunakan hasil pengujian dengan menghitung akurasi, presisi, *recall* dan *F1-score* untuk mengetahui keefektifan sistem. Rumus yang digunakan meliputi:

$$Accuracy = \frac{TP + TN}{TP + TN + FP\ FN}$$

Akurasi mengukur seberapa sering sistem membuat prediksi yang benar, baik dalam mendeteksi kejadian positif (TP) maupun negatif (TN), dari semua prediksi yang dibuat.

$$Precision = \frac{TP}{TP + FP}$$

Presisi menunjukkan seberapa banyak dari semua yang dideteksi sebagai positif oleh sistem benar-benar positif, sehingga mencerminkan tingkat keakuratan deteksi positif.

$$Recall = \frac{TP}{TP + FN}$$

Recall (*True Positive Rate* / Sensitivitas) mengukur seberapa baik sistem dapat menemukan semua kejadian positif yang benar-benar ada.

$$F1 - Score = 2 \,.\frac{Precision.Recall}{Precision + Recall}$$

F1 Score adalah rata-rata harmonis dari presisi dan recall, memberikan gambaran seimbang tentang performa sistem terutama ketika terdapat ketidak seimbangan antara data positif dan negatif.

Kesimpulan yang diambil dari hasil pengujian sistem dapat menjadi data untuk dijadikan sebagai kualitas hasil pengujian.