BAB II
TINJAUAN PUSTAKA

2.1 Kajian Penelitian Terdahulu

Beberapa penelitian menggunakan Wazuh sebagai alat monitoring jaringan untuk mendeteksi ancaman keamanan serta menganalisis aktivitas mencurigakan dan anomali dalam sistem. Oleh sebab itu untuk mendukung penelitian yang serupa, peneliti melakukan review pada beberapa jurnal untuk dijadikan acuan atau pedoman oleh peneliti pada tabel 1 berikut.

Tabel 1 Penelitian Terdahulu

No	Judul	Penulis	Tahun	Metode	Hasil
1.	IMPLEMENTASI WAZUH SIEM UNTUK MANAJEMEN LOG EVENT DI PESANTREN TEKNOLOGI INFORMASI DAN KOMUNIKASI JOMBANG	Faruq Aziz Saputra, Tubagus Rizky Dharmawan, April Rustianto	2024	Metode Eksperimen	Hasi yang didapatkan pada penelitian ini: 1. Implementasi Wazuh Berhasil. Wazuh terbukti efektif dalam mengelola dan memantau keamanan jaringan. 2. Sistem mampu mendeteksi dan merespons ancaman seperti Brute Force, DoS Attack, dan SQL Injection sesuai

					dengan harapan penelitian. 3. Sistem peringatan (alert system) berbasis bot Telegram memberikan respons real-time terhadap ancaman sehingga meningkatkan efisiensi dalam tindakan tanggap terhadap insiden keamanan.
2.	Design and Implementation of Security Gatway for IoT Devices Security	Marwan Alaa Hussein, Ekhlas Kadhum Hamza	2023	Metode Eksperimen	Hasil yang didapatkan dari peneitian ini : Raspberry Pi berhasil digunakan sebagai security gateway untuk melindungi perangkat IoT kecil dari ancaman eksternal. Wazuh berhasil mendeteksi serangan keamanan seperti Brute Force,

					DoS Attack, dan SQL Injection. Elasticsearch, Logstash, dan Kibana (ELK Stack) berhasil digunakan untuk memvisualisasikan log keamanan, Sistem dapat memberikan peringatan (alert) secara real-time untuk mempermudah respons terhadap insiden keamanan.sehingga lebih mudah memahami pola ancaman.
3.	Uji Kinerja Host-Based Intrution Detection SystemWAZUH terhadap Serangan Brute Force dan Dos	Oky Dwi Prasetyo, Primantara Hari Trisnawan, AdhityaBhawiyuga	2023	Metode Eksperimen	Hasil yang didapatkan dari penelitian ini : Wazuh mendeteksi serangan Brute Force dengan cepat dan akurat. Namun, Wazuh kurang efektif dalam mendeteksi

					serangan DoS karena tidak ada deteksi langsung dalam skenario pengujian. Keandalan Wazuh terbukti stabil dalam mendeteksi ancaman real-time untuk serangan Brute Force. Namun, Wazuh memerlukan optimalisasi atau konfigurasi tambahan untuk dapat mendeteksi serangan DoS dengan lebih baik.
4.	Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries	Md Rafiqul Islam, Raisa Rafique	2024	Metode Eksperimen	Hasil yang didapatkan dari penelitian ini : Sistem manajemen keamanan Wazuh berhasil mengidentifikasi laporan kegagalan autentikasi dan kerentanan. Selain itu, sistem ini menghasilkan

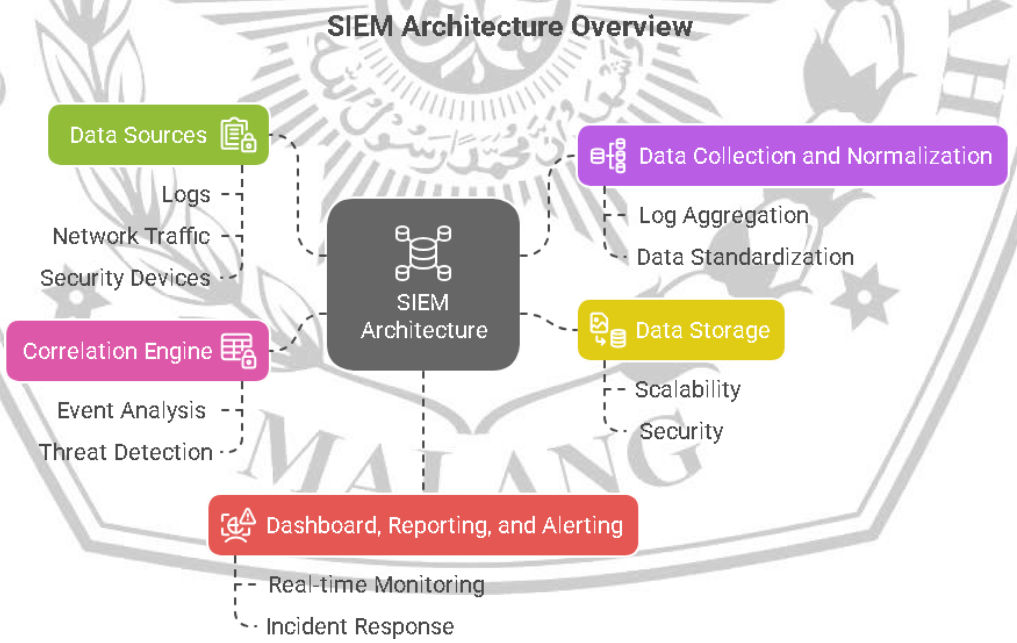
					laporan otomatis yang mengindikasikan 1 kerentanan kritis, 19 kerentanan tinggi, dan 5 kerentanan sedang. Wazuh juga menghasilkan laporan peristiwa keamanan dan pemantauan integritas. Implementasi Wazuh memastikan sistem manajemen keamanan yang kuat dan hemat biaya.
5	Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos	Muhammad Dehan Pratama, Fitri Nova, Deddy Prayama	2022	Metode Eksperimen	Hasil yang didapatkan dari penelitian ini : Wazuh terbukti mampu mendeteksi beberapa jenis serangan, terutama serangan Denial of Service (DoS) dengan menganalisis log event dan aktivitas

					mencurigakan pada server. Wazuh juga dapat mengidentifikasi percobaan akses tidak sah serta mendeteksi celah keamanan pada server yang berpotensi dimanfaatkan oleh penyerang. Terdapat juga beberapa jenis serangan yang kurang efektif dilacak oleh Wazuh, seperti serangan DoS yang lebih kompleks (DDoS) yang berasal dari berbagai sumber, eksploitasi zero-day yang belum terdokumentasi, serta serangan berbasis enkripsi atau steganografi yang menyembunyikan

					aktivitas berbahaya dalam lalu lintas terenkripsi.

2.2 SIEM

SIEM adalah teknologi yang memungkinkan untuk mendeteksi ancaman dan insiden keamanan melalui pengumpulan log secara *real-time* dan analisis data historis dari berbagai alat keamanan seperti (Router, IDS/IPS, UTM, Server, dll.). SIEM juga mendukung analisis dan investigasi insiden melalui analisis data historis dari berbagai macam tipe log dan sumber data yang berasal dari berbagai perangkat. Kemampuan inti dari teknologi SIEM adalah cakupan pengumpulan log yang luas dan kemampuan untuk mengkorelasikan dan menganalisis kejadian di berbagai sumber yang berbeda yang terdapat pada gambar 1.



Gambar 1 Arsitektur SIEM

a. Data sources

Informasi yang dikumpulkan dari berbagai sumber dalam jaringan dan infrastruktur menjadi elemen utama dalam sistem SIEM. Sumber-sumber ini mencakup perangkat seperti *firewall*, sistem deteksi dan pencegahan intrusi (IDS/IPS), program antivirus, serta log dari sistem operasi, *database*, server web, dan aplikasi maupun layanan *cloud*. Selain itu, data yang berasal dari perangkat pengguna seperti komputer, laptop, dan perangkat mobile, serta log akses dan autentikasi pengguna.[13]

b. Data collection and normalization

SIEM mengumpulkan data dari berbagai sumber melalui agen, API, atau penerusan log. Karena format data tiap sumber berbeda, data tersebut harus melalui proses normalisasi dan penguraian. Umumnya, SIEM menyediakan pengurai bawaan, namun beberapa juga mendukung pengurai kustom untuk format yang belum dikenal. Normalisasi bertujuan menyatukan data dalam format seragam guna mendukung analisis yang konsisten.[13]

c. Data storage

Setelah dinormalisasi, data akan disimpan dalam repositori yang terpusat. Beberapa platform SIEM memanfaatkan sistem basis data relasional (RDBMS) seperti MySQL, PostgreSQL, atau Microsoft SQL Server untuk menyimpan informasi peristiwa yang memiliki struktur tetap. Sementara itu, solusi lainnya menggunakan basis data NoSQL seperti MongoDB atau Elasticsearch untuk menangani log yang bersifat semi-terstruktur atau tidak terstruktur. Penyimpanan secara terpusat ini memungkinkan pelaksanaan pencarian, analisis, dan pelaporan secara lebih efisien. Untuk menyimpan data keamanan historis dalam volume besar, biasanya digunakan solusi pengumpulan data seperti Amazon Redshift atau Snowflake.[13]

d. Corellation engine

Mesin korelasi digunakan untuk mengevaluasi data yang dikumpulkan dengan tujuan mendeteksi pola dan kemungkinan terjadinya insiden keamanan melalui pengaitan berbagai peristiwa dari sejumlah sumber yang berbeda. Beragam teknik dapat diterapkan dalam proses korelasi ini, antara lain

pendekatan statistik, penalaran berbasis aturan, penalaran berbasis kasus, penalaran berbasis model, penalaran Bayesian, serta metode dengan pendekatan grafis.[13]

e. Dashboard, reporting and alerting

SIEM menyajikan dasbor yang dirancang untuk memantau kondisi keamanan organisasi secara langsung dan terus-menerus. Umumnya, dasbor ini menampilkan data dalam bentuk visual seperti grafik, bagan, dan widget interaktif. Sistem juga memungkinkan pembuatan laporan secara otomatis dalam interval tertentu maupun atas permintaan, yang berguna untuk kebutuhan kepatuhan, investigasi insiden, serta pelaporan kepada pihak eksekutif. Selain itu, dasbor akan menampilkan peringatan yang dihasilkan dari proses korelasi data saat terdeteksi adanya potensi ancaman atau aktivitas mencurigakan. Peringatan ini dapat diatur untuk mengirim notifikasi melalui email, SMS, atau terintegrasi dengan sistem respons insiden. Biasanya, setiap peringatan diklasifikasikan menurut tingkat urgensinya guna mempermudah penentuan prioritas dalam proses penanganan insiden.[13]

2.3 Wazuh

Wazuh merupakan perangkat lunak keamanan open-source yang berfungsi sebagai sistem deteksi berbasis host (endpoint). Platform ini mengintegrasikan kemampuan XDR (Extended Detection and Response) dan SIEM (Security Information and Event Management) untuk melakukan berbagai fungsi, seperti analisis log, pendeteksian intrusi dan malware, pemantauan integritas berkas, penilaian konfigurasi berbasis standar industri, identifikasi kerentanan, serta dukungan terhadap kepatuhan keamanan. Wazuh mampu menghasilkan peringatan secara real-time dan melakukan tindakan respons otomatis.

Selain itu, Wazuh memberikan tingkat visibilitas keamanan yang lebih komprehensif dengan memantau aktivitas pada host di level sistem operasi maupun aplikasi. Secara arsitektural, Wazuh terdiri dari tiga komponen utama—Wazuh Indexer, Wazuh Server, dan Wazuh Dashboard—serta komponen agen yang terpasang pada endpoint sebagai Wazuh Agent.

a. Wazuh Indexer

Wazuh Indexer adalah komponen mesin pencarian yang berfungsi untuk mengelola proses pengindeksan dan penyimpanan pesan yang dikirim oleh Wazuh Server. Keberadaan indexer memungkinkan proses pencarian data, pemrosesan informasi, dan analisis log menjadi lebih cepat dan efisien. Seluruh data yang diterima disimpan dalam bentuk dokumen JSON, di mana setiap indeks terdiri dari sekumpulan dokumen yang memiliki karakteristik atau struktur serupa.

b. Wazuh Server

Wazuh Server berperan sebagai pusat pemrosesan yang menganalisis data yang dikirimkan oleh Wazuh Agent. Informasi tersebut diproses melalui decoder dan rule yang didukung oleh threat intelligence guna mengidentifikasi potensi ancaman. Selain berfungsi untuk mendeteksi, Wazuh Server juga bertanggung jawab dalam pengelolaan Wazuh Agent, mulai dari konfigurasi, pemantauan, hingga proses pembaruan (upgrade) agent.

c. Wazuh Dashboard

Wazuh Dashboard merupakan antarmuka berbasis web yang digunakan untuk melakukan visualisasi data serta mendukung proses analisis keamanan. Melalui dashboard ini, pengguna dapat melihat berbagai informasi seperti security events, tingkat kepatuhan regulasi, kerentanan aplikasi yang terdeteksi, hasil pemantauan integritas berkas, penilaian konfigurasi, hingga aktivitas monitoring pada lingkungan cloud. Selain fungsi visualisasi, Wazuh Dashboard juga menyediakan fasilitas untuk mengelola konfigurasi sistem Wazuh serta memantau status komponen yang berjalan.

d. Wazuh Agent

Wazuh Agent diterapkan pada perangkat endpoint seperti Linux, Windows, macOS, Solaris, AIX, dan berbagai sistem operasi lainnya. Agen ini menyediakan kemampuan deteksi, pencegahan, serta respons terhadap ancaman keamanan. Sebagai komponen yang bersifat multi-platform, Wazuh Agent berjalan langsung pada endpoint yang ingin dipantau dan berfungsi

mengirimkan data ke Wazuh Server hampir secara real-time melalui kanal komunikasi yang terenkripsi dan terautentikasi. Agen ini dirancang agar mampu melakukan pemantauan pada beragam jenis endpoint tanpa memberikan dampak signifikan terhadap performa perangkat. Wazuh Agent mendukung sistem operasi populer dan umumnya hanya membutuhkan sekitar 35 MB RAM untuk dapat beroperasi secara optimal.