

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat pada era digital saat ini telah membawa berbagai kemudahan dalam mendukung aktivitas organisasi dan operasional sistem informasi. Namun demikian, pertumbuhan ini juga disertai dengan meningkatnya ancaman terhadap keamanan jaringan. Aktivitas seperti *port scanning* (Coyle, 2024), *SSH brute force* (Fitra Pradana, 2023), dan *SQL injection* (Elu, 2013) merupakan pola serangan yang umum ditemukan pada infrastruktur jaringan dan aplikasi web, yang dapat mengganggu ketersediaan layanan, merusak integritas data, hingga menyebabkan kebocoran informasi. Kondisi ini menuntut organisasi untuk memiliki sistem keamanan yang tidak hanya mampu melakukan deteksi secara menyeluruh, tetapi juga memberikan respon cepat dan efektif terhadap setiap insiden keamanan yang terjadi (Sarker et al., 2023).

Salah satu pendekatan yang umum digunakan dalam pengelolaan keamanan jaringan adalah penerapan *Security Information and Event Management* (SIEM). Teknologi ini berfungsi untuk mengumpulkan, menganalisis, dan memantau log keamanan dari berbagai perangkat dalam jaringan secara terpusat (Kamal, 2022). Dalam proyek akhir ini, Wazuh digunakan sebagai platform SIEM berbasis *open source* yang berfungsi untuk mendeteksi berbagai aktivitas mencurigakan secara *real-time* (Azzah, 2024). Akan tetapi, penelitian terdahulu yang dilakukan di lingkungan Politeknik Caltex Riau menunjukkan bahwa meskipun Wazuh efektif dalam memantau *server* dan menyajikan data serangan dalam log, Wazuh tidak dapat secara otomatis menanggapi serangan keamanan dan masih memerlukan integrasi dengan sistem lain untuk menanggapi serangan tersebut (Zahira, 2023). Dengan kata lain, SIEM pada umumnya hanya berperan sebagai alat *monitoring* dan belum memiliki kemampuan untuk merespons ancaman secara otomatis, sehingga masih dibutuhkan intervensi manual dari administrator untuk menindaklanjuti setiap insiden.

Untuk mengatasi keterbatasan tersebut, dibutuhkan sistem tambahan yang mampu melakukan otomatisasi respon terhadap insiden keamanan. Dalam hal ini,

digunakan Shuffle SOAR (*Security Orchestration, Automation, and Response*), sebuah platform *open source* yang memungkinkan integrasi dan orkestrasi berbagai proses keamanan secara otomatis melalui pembuatan *workflow* (Habibie, 2024). Shuffle SOAR akan menerima *alert* dari Wazuh dan menjalankan aksi tertentu, seperti pemblokiran IP, secara otomatis berdasarkan aturan yang telah ditentukan.

Dalam sistem ini, tindakan pemblokiran dilakukan oleh FortiGate, sebuah perangkat *Next-Generation Firewall* (NGFW) yang memiliki kemampuan mendalam dalam pencegahan dan penanggulangan ancaman, seperti melalui fitur *Intrusion Prevention System* (IPS), *Threat Intelligence*, serta *Traffic Filtering* (Fortigate, 2025). Penelitian sebelumnya juga telah membuktikan efektivitas FortiGate dalam mendeteksi dan memblokir serangan jaringan seperti ICMP *Flooding* dan *Port Scanning* pada lingkungan laboratorium kampus (Jaya dkk., 2021). Dengan mengintegrasikan komponen Wazuh, Shuffle, dan FortiGate diharapkan tercipta sistem keamanan jaringan yang tidak hanya mampu mendeteksi ancaman, tetapi juga meresponsnya secara otomatis dan efisien tanpa memerlukan keterlibatan manual yang berkepanjangan.

Beberapa penelitian terdahulu di lingkungan Politeknik Caltex Riau telah membahas komponen-komponen keamanan jaringan secara terpisah, seperti implementasi Wazuh sebagai SIEM tunggal tanpa kemampuan respons otomatis (Zahira, 2023), maupun analisis performa FortiGate sebagai *firewall* dalam menghadapi serangan tertentu tanpa keterhubungan dengan sistem deteksi berbasis log (Ibrahim dkk., 2023). Uraian mengenai perkembangan penelitian yang lebih mutakhir (*state of the art*) pada bidang integrasi SIEM dan SOAR, serta celah penelitian yang menjadi dasar penelitian ini, disajikan masing-masing pada Sub Bab 1.2 dan Sub Bab 1.3.

1.2 State of the Art

Penelitian mengenai integrasi SIEM dan SOAR telah berkembang untuk mendukung otomatisasi deteksi dan respons terhadap insiden keamanan. Sagita (2024) mengintegrasikan Wazuh, Suricata, Shuffle, dan Iris untuk mengotomatisasi respons terhadap beberapa jenis serangan, seperti *brute force*, *reconnaissance*, *denial of service*, *SQL injection*, dan *cross-site scripting*. Hasil penelitian menunjukkan bahwa integrasi SIEM dan SOAR dapat mendukung proses deteksi

dan respons secara otomatis.

Penelitian (Ridwan & Yudi Kurniawan, 2025) juga membahas penerapan integrasi SIEM dan SOAR dalam otomatisasi respons keamanan. Penelitian tersebut menunjukkan bahwa orkestrasi antara sistem deteksi dan mekanisme respons dapat mengurangi ketergantungan terhadap intervensi manual.

Berdasarkan penelitian terdahulu tersebut, penelitian ini menerapkan integrasi Wazuh sebagai SIEM, Shuffle sebagai SOAR, dan FortiGate sebagai *firewall* untuk melakukan respons otomatis terhadap serangan *SSH Brute Force*, *Port Scanning*, dan *SQL Injection*. Selain integrasi tersebut, penelitian ini menerapkan mekanisme validasi pada *workflow* sebelum proses pemblokiran dijalankan serta melakukan evaluasi berdasarkan *response time*, *detection accuracy*, *blocking success rate*, dan *false positive rate*.

1.3 Research Gap

Berdasarkan penelitian terdahulu, integrasi SIEM dan SOAR telah diterapkan untuk mendukung deteksi dan respons terhadap insiden keamanan secara otomatis. Namun, masih terdapat perbedaan pada perangkat eksekutor, jenis serangan yang diuji, serta metode evaluasi kinerja sistem. Penelitian terdahulu yang ditinjau belum secara khusus mengintegrasikan Wazuh, Shuffle, dan FortiGate untuk menangani *SSH Brute Force*, *Port Scanning*, dan *SQL Injection* dalam satu alur respons otomatis.

Selain itu, evaluasi terhadap mekanisme otomatisasi belum secara khusus mencakup *response time*, *detection accuracy*, *blocking success rate*, dan *false positive rate* secara terukur. Oleh karena itu, penelitian ini mengembangkan integrasi Wazuh, Shuffle, dan FortiGate dengan menerapkan validasi berbasis *rule ID* sebelum proses pemblokiran serta melakukan pengujian kinerja sistem secara kuantitatif.

1.4 Kontribusi Penelitian

Berdasarkan celah penelitian yang telah diuraikan, penelitian ini memberikan beberapa kontribusi sebagai berikut:

1. Merancang dan mengimplementasikan integrasi *end-to-end* antara Wazuh sebagai SIEM, Shuffle sebagai SOAR, dan FortiGate sebagai *firewall*

enterprise dengan mekanisme manajemen kebijakan berbasis *address group*, yang belum ditemukan pada penelitian SIEM–SOAR terdahulu (Sagita, 2024; Ridwan & Kurniawan, 2025).

2. Mengembangkan *custom rule* deteksi pada Wazuh (rule ID 100100, 100101, dan 100201) yang disesuaikan dengan karakteristik masing-masing pola serangan SQL Injection berbasis pola *endpoint*, SSH Brute Force dan Port Scanning berbasis *correlation rule* dengan ambang *frequency* dan *timeframe* tertentu sehingga tindakan respons tidak dipicu oleh kejadian tunggal.
3. Menerapkan mekanisme validasi eksplisit pada tahap orkestrasi berupa *condition filter* di workflow Shuffle, yang menyaring alert berdasarkan identitas rule sebelum diteruskan ke tahap pemblokiran suatu *decision point* yang belum diterapkan pada penelitian SIEM–SOAR berbasis Wazuh dan Shuffle sebelumnya.
4. Melakukan pengujian kuantitatif sistematis terhadap empat aspek kinerja sistem *response time*, *detection accuracy*, *blocking success rate*, dan *false positive rate* melalui sepuluh kali pengulangan pada setiap skenario serangan, sehingga evaluasi tidak terbatas pada pembuktian keberhasilan fungsional semata.
5. Memberikan analisis reflektif mengenai batasan metodologis dan risiko operasional dari setiap mekanisme yang diimplementasikan, sebagai acuan bagi pengembangan lebih lanjut menuju kesiapan penerapan pada lingkungan produksi.

1.5 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka perumusan masalah dalam penelitian ini adalah diperlukan suatu sistem keamanan jaringan yang tidak hanya mampu mendeteksi ancaman secara real-time, tetapi juga dapat memberikan respons otomatis terhadap insiden keamanan tanpa keterlibatan manual yang berkepanjangan. Selain itu, dibutuhkan evaluasi terhadap efektivitas sistem dalam mendeteksi dan merespons berbagai jenis serangan jaringan, seperti port scanning, SSH brute force, dan SQL injection, dalam lingkungan virtual. Di samping itu, perlu diidentifikasi dan diatasi berbagai tantangan teknis yang muncul selama proses integrasi dan otomatisasi sistem keamanan berbasis open source dengan perangkat firewall.

1.6 Batasan Masalah

Agar ruang lingkup penelitian tidak terlalu luas, batasan masalah yang diterapkan adalah sebagai berikut:

6. Jenis serangan yang disimulasikan dibatasi pada port scanning, SSH brute force, dan SQL injection.
7. Penelitian hanya berfokus pada proses deteksi dan automasi respon, tidak membahas aspek keamanan fisik, enkripsi data, atau analisis biaya.

1.7 Tujuan dan Manfaat

1.7.1 Tujuan

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang dan mengimplementasikan sistem keamanan jaringan berbasis open source yang mampu melakukan deteksi ancaman secara real time serta memberikan respon otomatis terhadap insiden keamanan, guna mengurangi keterlibatan manual dari administrator
2. Mengintegrasikan platform Wazuh, Shuffle, dan FortiGate ke dalam satu kesatuan sistem yang mampu mendeteksi serta merespons ancaman jaringan secara efisien dan terotomatisasi.
3. Menguji efektivitas sistem yang dibangun dalam mendeteksi dan merespons serangan jaringan, khususnya jenis serangan port scanning, SSH brute force, dan SQL injection, dalam lingkungan virtual yang dikendalikan.

1.7.2 Manfaat

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Memberikan solusi sistem keamanan jaringan yang terotomatisasi dan mampu merespons ancaman secara cepat.
2. Membantu administrator jaringan dalam mengurangi ketergantungan pada tindakan manual saat menangani insiden keamanan.
3. Meningkatkan efisiensi operasional dalam penanganan insiden keamanan jaringan, dengan mengurangi ketergantungan terhadap intervensi manual dan mempercepat waktu respon terhadap serangan siber yang terjadi.