BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi yang semakin pesat telah membawa transformasi besar terhadap cara organisasi menjalankan operasionalnya. Ketergantungan terhadap sistem digital, jaringan komputer, serta konektivitas internet menyebabkan meningkatnya risiko terhadap ancaman siber yang semakin kompleks dan sulit diprediksi. Menurut Tolossa [1], pertumbuhan serangan siber yang signifikan menunjukkan bahwa keamanan tidak lagi hanya bergantung pada infrastruktur teknologi, tetapi juga pada kesiapan organisasi dalam membangun sistem pertahanan siber yang adaptif. Di Indonesia sendiri, peningkatan insiden kebocoran data dan serangan terhadap institusi publik menegaskan lemahnya kesiapan nasional dalam menghadapi ancaman digital yang bersifat dinamis [2]. Oleh karena itu, pengembangan sistem keamanan yang mampu melakukan deteksi dini terhadap aktivitas anomali menjadi kebutuhan penting bagi organisasi dan individu yang bergantung pada sistem berbasis TI.

Salah satu pendekatan yang efektif dalam memperkuat keamanan digital adalah melalui penerapan *Intrusion Detection System* (IDS), khususnya jenis *Host-based Intrusion Detection System* (HIDS). Sistem ini beroperasi langsung pada host untuk memantau log aktivitas, integritas file, dan perubahan konfigurasi yang mencurigakan. Penelitian Deshpande et al. [3] menjelaskan bahwa HIDS mampu memberikan deteksi intrusi yang lebih cepat dengan menganalisis jejak sistem secara selektif, terutama pada proses-proses yang gagal, sehingga beban komputasi dapat diminimalkan tanpa mengurangi akurasi deteksi. Dalam konteks lingkungan internal, penerapan HIDS menjadi sangat relevan karena dapat memberikan lapisan pertahanan tambahan terhadap ancaman lokal seperti *brute force login*, *file modification attack*, maupun aktivitas *malware persistence* yang tidak terdeteksi oleh solusi perimeter seperti firewall atau NIDS.

Wazuh sebagai platform open-source untuk deteksi dan manajemen keamanan menawarkan kapabilitas HIDS yang komprehensif, mencakup *log analysis*, *file integrity monitoring*, serta *real-time alerting*. Implementasi Wazuh pada sistem internal memungkinkan proses pemantauan yang terpusat dan transparan terhadap aktivitas host, tanpa memerlukan infrastruktur cloud.

Berdasarkan penelitian Basit et al. [4], integrasi komponen Wazuh dengan sistem organisasi memberikan kemampuan deteksi terhadap serangan seperti *port scanning*, *denial of service*, dan eksploitasi berbasis skrip. Dalam simulasi implementasi pada lingkungan lokal, konfigurasi Wazuh dapat dioptimalkan untuk mengirimkan notifikasi otomatis melalui *Simple Mail Transfer Protocol* (SMTP), sehingga setiap aktivitas anomali dapat segera direspon. Pendekatan ini mencerminkan integrasi sederhana antara deteksi host dan mekanisme *automated response*, yang sejalan dengan konsep *security automation* sebagaimana dikemukakan oleh Mohammad dan Lakshmisri [5].

Otomatisasi dalam sistem keamanan berperan penting untuk meningkatkan efisiensi deteksi dan respons terhadap ancaman. Mekanisme manual dalam proses eskalasi sering kali menyebabkan keterlambatan penanganan, terutama ketika volume notifikasi tinggi. Dengan penerapan otomasi, sistem dapat melakukan triase dan mengirimkan peringatan secara mandiri tanpa campur tangan manusia. Penelitian Mohammad dan Lakshmisri [5] menegaskan bahwa automasi keamanan mampu mengurangi kesalahan manusia serta mempercepat proses pengambilan keputusan. Sementara itu, Mahardika et al. [6] menyoroti pentingnya kesadaran keamanan siber di tingkat pengguna agar proses deteksi dan mitigasi dapat berjalan efektif. Oleh karena itu, implementasi simulasi HIDS berbasis Wazuh dengan kemampuan pengiriman notifikasi otomatis tidak hanya memperkuat sistem deteksi, tetapi juga menjadi langkah awal dalam membangun budaya responsif terhadap ancaman keamanan di lingkungan sistem internal.

1.2 Maksud dan Tujuan Kerja Magang

Maksud utama dari kegiatan magang ini adalah melakukan eksplorasi mendalam terhadap konsep dan implementasi *Host-based Intrusion Detection System* (HIDS) dengan memanfaatkan platform Wazuh sebagai sarana pembelajaran teknis dan praktis dalam konteks keamanan sistem informasi. Aktivitas ini berfokus pada pengembangan prototipe sistem otomatisasi pengiriman peringatan (*alert automation*) dari HIDS, yang dirancang untuk mensimulasikan proses deteksi serta notifikasi terhadap aktivitas anomali pada host internal. Dengan pendekatan ini, sistem diharapkan mampu memberikan pemahaman komprehensif mengenai mekanisme deteksi berbasis host serta keterkaitannya dengan proses eskalasi insiden dalam *Security Operations Center* (SOC).

Tujuan dari kegiatan magang ini adalah merancang dan

mengimplementasikan prototipe sistem otomatisasi peringatan keamanan berbasis *Host-based Intrusion Detection System* (HIDS) menggunakan Wazuh dalam lingkungan simulasi *Security Operations Center* (SOC). Kegiatan ini bertujuan untuk memahami arsitektur dan alur kerja HIDS, mulai dari proses pengumpulan, analisis, hingga korelasi *log* aktivitas pada sistem host yang menghasilkan *alert* keamanan. Melalui implementasi tersebut, dilakukan verifikasi terhadap mekanisme konfigurasi HIDS dalam menghasilkan *alert* berdasarkan kondisi tertentu pada sistem host. Penggunaan *rule* sederhana, seperti deteksi status *agent started* dan *agent stopped*, difokuskan untuk memastikan bahwa alur deteksi dan pengiriman peringatan otomatis dapat berjalan dengan baik. Dengan pendekatan ini, prototipe yang dikembangkan memberikan gambaran awal mengenai peran sistem peringatan otomatis dalam mendukung aktivitas monitoring di lingkungan SOC, serta membuka peluang pengembangan lebih lanjut untuk penerapan *rule* deteksi pada skenario dan aktivitas keamanan yang lebih beragam.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Program magang dilaksanakan di Defenxor pada divisi SOC yang berada di bawah pilar *Defenxor Intelligence Managed Security* (DIMS). Kegiatan berlangsung selama satu tahun, dimulai pada 3 Februari 2025 hingga 2 Februari 2026. Seluruh aktivitas dilakukan secara *onsite* dengan sistem kerja penuh waktu di kantor pusat operasional yang berlokasi di Graha BIP lantai 6, Jalan Jenderal Gatot Subroto Kavling 23, Karet Semanggi, Jakarta Selatan.

Setelah menyelesaikan tahap pelatihan dasar, peserta magang menjalani sistem kerja *shift* yang diterapkan di lingkungan SOC. Pembagian jadwal dibagi menjadi dua sayap, sayap kiri (Minggu–Rabu) dan sayap kanan (Rabu–Sabtu), dengan rotasi yang berganti setiap minggu. Penjadwalan mencakup tiga sesi utama, yakni *Early Shift* (05.00–15.00 WIB), *Mid Shift* (10.00–20.00 WIB), dan *Late Shift* (19.30–05.30 WIB). Penerapan tiga pola *shift* tersebut memastikan agar operasional SOC dapat berlangsung selama 24 jam penuh.