BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan sistem informasi saat ini menghadapi tantangan yang semakin kompleks, khususnya terkait upaya penyusupan yang memanfaatkan manipulasi berkas pada server atau *endpoint*. Salah satu indikator penting terjadinya kompromi sistem adalah perubahan pada integritas berkas, baik berupa penambahan (*added*), modifikasi (*modified*), maupun penghapusan (*deleted*). Perubahan yang tidak sah pada berkas kritis dapat menimbulkan berbagai risiko, seperti pemasangan *malware*, penyisipan *backdoor*, pengubahan konfigurasi keamanan, hingga penghapusan log yang dapat menghilangkan jejak serangan. Bentuk pelanggaran tersebut mencakup manipulasi data (*data tampering*), perusakan data (*data destruction*), modifikasi tanpa otorisasi, penyisipan kode berbahaya, kelalaian pengguna, serta penghapusan berkas secara tidak sengaja [1].

Dalam konteks operasional *Security Operations Center* (SOC), kemampuan untuk memonitor dan mengidentifikasi perubahan berkas secara *real-time* menjadi bagian penting dari mekanisme deteksi dini. *File Integrity Monitoring* (FIM) merupakan pendekatan yang digunakan untuk memantau aktivitas pada berkas dan direktori tertentu, sehingga indikasi ancaman dapat dikenali sejak tahap awal sebelum berkembang menjadi insiden keamanan yang lebih luas [1]. Melalui pemantauan ini, analis SOC dapat mengidentifikasi aktivitas tidak wajar, seperti perubahan konfigurasi sistem, pembuatan berkas mencurigakan, atau penghapusan file penting yang berpotensi mengindikasikan adanya pelanggaran keamanan.

Wazuh sebagai platform *open-source security monitoring* menyediakan fitur *Host-based Intrusion Detection System* (HIDS) yang dilengkapi dengan modul *File Integrity Monitoring*. Melalui proses integrasi Wazuh HIDS dengan platform SIEM, perubahan berkas yang terdeteksi dapat dicatat, diklasifikasikan, dan dianalisis berdasarkan jenis aktivitas seperti *added*, *modified*, dan *deleted*. Mekanisme ini memungkinkan dilakukan simulasi skenario perubahan berkas yang berpotensi mengindikasikan aktivitas berbahaya, serta memberikan gambaran mengenai bagaimana data hasil pemantauan diproses dalam alur kerja SOC.

Namun demikian, efektivitas pemantauan integritas berkas sangat dipengaruhi oleh konfigurasi sistem, cakupan direktori yang dipantau, serta

ketepatan aturan deteksi yang digunakan. Oleh karena itu, diperlukan analisis terhadap proses integrasi Wazuh HIDS dalam melakukan simulasi *File Integrity Monitoring* guna memahami sejauh mana sistem mampu mendeteksi dan menyajikan informasi perubahan berkas yang relevan bagi kebutuhan analisis keamanan.

Berdasarkan latar belakang tersebut, kegiatan magang ini berfokus pada analisis integrasi Wazuh HIDS sebagai sistem simulasi untuk mengevaluasi kemampuan *File Integrity Monitoring* dalam mendeteksi perubahan berkas yang berpotensi membahayakan keamanan sistem.

1.2 Maksud dan Tujuan Kerja Magang

Kegiatan magang ini bertujuan untuk menganalisis integrasi Wazuh *Host Intrusion Detection System* (HIDS) dalam mensimulasikan mekanisme *File Integrity Monitoring* sebagai bagian dari operasional *Security Operations Center* (SOC). Analisis dilakukan melalui proses konfigurasi dan integrasi modul *File Integrity Monitoring* pada Wazuh HIDS, serta pengamatan terhadap hasil deteksi perubahan berkas pada lingkungan simulasi.

Secara spesifik, manfaat dari kegiatan magang ini meliputi:

- Memberikan pemahaman praktis mengenai proses integrasi dan analisis Wazuh HIDS, khususnya modul *File Integrity Monitoring*, dalam mendukung aktivitas *security monitoring*.
- Mengembangkan kemampuan analisis terhadap perubahan berkas yang berpotensi menjadi indikator kompromi sistem, termasuk proses verifikasi dan interpretasi *alert* FIM.
- Memperoleh pengalaman dalam mengevaluasi kinerja mekanisme *File Integrity Monitoring* sebagai bagian dari deteksi dini serta pendukung proses *incident response* pada lingkungan simulasi SOC.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Pelaksanaan magang di PT Defender Nusa Semesta berlangsung selama satu tahun, mulai 3 Februari 2025 hingga 2 Februari 2026. Kegiatan magang dijalankan empat hari setiap minggu dengan total durasi 40 jam. Seluruh aktivitas dilakukan di kantor PT Defender Nusa Semesta yang berlokasi di Graha BIP lantai 6, Jalan

Gatot Subroto, Jakarta Selatan, yang menjadi pusat operasional *Security Operations Center* (SOC).

Setiap hari kerja berlangsung selama 10 jam, termasuk waktu istirahat maksimal 2 jam. Pengaturan ini diterapkan untuk menyesuaikan kebutuhan operasional pemantauan keamanan yang berjalan secara berkesinambungan. Untuk mendukung monitoring selama 24 jam, sistem kerja dibagi menjadi dua kelompok, yaitu Sayap Kiri (Minggu–Rabu) dan Sayap Kanan (Rabu–Sabtu). Selain itu, pembagian shift terdiri dari tiga kategori, yakni *early shift*, *mid shift*, dan *late shift*, yang memastikan proses deteksi dan respons insiden tetap berjalan secara *real-time*.

Kegiatan operasional SOC sepenuhnya dilaksanakan secara *work from office* (WFO). Dalam pelaksanaannya, pengajuan *day off* tidak dapat dilakukan secara mendadak karena sistem shift membutuhkan kesinambungan antarpetugas. Oleh karena itu, pengajuan *day off* harus diajukan setelah memperoleh pengganti yang bersedia mengisi jadwal pada shift terkait. Selain itu, setiap hari Rabu dijadwalkan *weekly meeting* yang dihadiri seluruh personel SOC untuk membahas evaluasi mingguan, kendala operasional, dan pembaruan terkait aktivitas pemantauan.