BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi telah memberikan banyak kemudahan, namun juga diiringi dengan peningkatan ancaman keamanan siber. Berbagai serangan seperti *malware*, pencurian data, dan eksploitasi sistem jaringan semakin sering terjadi dan dapat menimbulkan kerugian signifikan bagi individu maupun organisasi. Oleh karena itu, keamanan informasi menjadi faktor penting yang harus diperhatikan agar data tetap terjaga kerahasiaan, integritas, serta ketersediaannya. Kompleksitas infrastruktur teknologi yang terus berkembang menyebabkan ancaman siber juga semakin beragam dan membutuhkan langkah mitigasi yang lebih terstruktur [1].

Meningkatnya ancaman keamanan informasi mendorong organisasi untuk membangun mekanisme pemantauan yang lebih komprehensif. Salah satu pendekatan yang umum diterapkan adalah pembentukan *Security Operations Center* (SOC) sebagai pusat analisis dan respons terhadap insiden keamanan. Untuk mendukung fungsi tersebut, SOC biasanya dilengkapi dengan *Security Information and Event Management* (SIEM), yang bertugas mengumpulkan, mengkorelasikan, dan menganalisis event log dari berbagai perangkat secara real-time untuk mendeteksi anomali dan pola serangan [2]. Meski demikian, efektivitas SIEM dalam menghasilkan peringatan yang bermakna sangat bergantung pada penerapan kebijakan keamanan — seperti kontrol akses, autentikasi, dan prosedur respons insiden — agar jumlah false positive dapat diminimalkan dan alert dapat fokus pada ancaman yang relevan [2].

Meskipun SIEM efektif dalam menganalisis data log dari berbagai sumber, sistem ini membutuhkan informasi yang lebih mendalam dari sisi host agar deteksi ancaman dapat dilakukan secara lebih komprehensif. *Host Intrusion Detection System* (HIDS) berperan penting dalam memantau aktivitas pada perangkat tertentu, sehingga mampu mendeteksi penyusupan maupun perilaku mencurigakan yang mungkin tidak terlihat pada level jaringan. Dengan adanya HIDS, akan didapatkan peringatan lebih dini mengenai aktivitas berbahaya di host, yang kemudian dapat diintegrasikan ke dalam SIEM untuk menghasilkan analisis keamanan yang lebih menyeluruh [3].

Dalam konteks magang di PT Defender Nusa Semesta, aktivitas yang dilakukan sehari-hari adalah pemantauan keamanan sebagai analis SOC. Sebagai salah satu nilai knowledge-improvement pada perusahaan, dibuat sebuah prototipe *Host Intrusion Detection System* (HIDS) sebagai simulasi guna memahami alur kerja deteksi intrusi serta integrasinya dengan SIEM pada lingkungan SOC. HIDS dapat diimplementasikan untuk mendeteksi aktivitas berbahaya pada host, di mana sistem ini menghasilkan peringatan yang membantu dalam melakukan tindakan mitigasi [4]. Dengan demikian, prototipe ini tidak hanya menjadi media pembelajaran, tetapi juga memberikan gambaran nyata tentang bagaimana HIDS berkontribusi dalam mendukung efektivitas monitoring keamanan.

1.2 Maksud dan Tujuan Kerja Magang

Maksud dari program magang tahap kedua adalah memperdalam pemahaman mengenai operasional SOC melalui pengembangan sebuah prototipe *Host Intrusion Detection System* (HIDS) yang disimulasikan sebagai bagian dari sistem security monitoring. Prototipe ini dirancang untuk meniru fungsi deteksi aktivitas berbahaya pada host dan integrasinya dengan SIEM, sehingga memberikan gambaran nyata mengenai pemanfaatan data dari endpoint untuk analisis keamanan yang lebih komprehensif. Implementasi prototipe ini sekaligus menjadi sarana penerapan konsep-konsep *cybersecurity* yang telah diperoleh dalam perkuliahan di Universitas Multimedia Nusantara, serta memperluas pengalaman magang di PT Defender Nusa Semesta.

Tujuan pelaksanaan proyek ini adalah mengembangkan keterampilan teknis dalam merancang, mengonfigurasi, dan menguji sistem deteksi intrusi berbasis host, serta memahami peranannya dalam mendukung efektivitas operasional SOC. Melalui proyek ini diharapkan dapat diperoleh pemahaman yang lebih mendalam mengenai *security monitoring*, sekaligus menekankan aspek perancangan sistem keamanan sebagai simulasi akademik. Dengan demikian, program magang tahap kedua ini berkontribusi dalam peningkatan kompetensi di bidang *cybersecurity* serta mendukung tercapainya standar keamanan informasi yang lebih baik.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Program magang di PT Defender Nusa Semesta (DNS) dijalankan dalam beberapa tahap sesuai ketentuan perusahaan. Tahap kedua magang dilaksanakan

pada Juli hingga November 2025, dengan posisi sebagai security analyst intern. Kegiatan magang dijalankan empat hari setiap minggu dengan total 40 jam kerja, menggunakan sistem shifting. Seluruh aktivitas magang dilaksanakan di Graha BIP lantai 6, Jalan Gatot Subroto, Jakarta Selatan, yang menjadi lokasi operasional SOC perusahaan.

Pelaksanaan magang mengikuti sistem pembagian kerja yang disebut sistem sayap. Dalam skema ini, tim dibagi menjadi dua kelompok: sayap kiri yang bertugas dari Minggu hingga Rabu, dan sayap kanan yang bekerja dari Rabu hingga Sabtu. Hari Rabu ditetapkan sebagai hari penting karena seluruh anggota SOC berkumpul untuk mengikuti *weekly meeting* guna melakukan evaluasi serta menyampaikan *update* mingguan. Selain pembagian kelompok, sistem kerja juga diatur dengan tiga jenis *shift*, yaitu *early shift*, *mid shift*, dan *late shift*, sehingga kegiatan *monitoring* dan penanganan insiden keamanan dapat berjalan penuh 24 jam secara *real-time*.