BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan siber merupakan aspek krusial dalam dunia teknologi informasi, terutama bagi perusahaan yang bergantung pada infrastruktur digital untuk menjalankan operasional bisnisnya. Ancaman siber seperti serangan phishing, malware, dan eksploitasi kerentanan sistem terus meningkat dari tahun ke tahun. Berdasarkan laporan dari Cybersecurity Ventures, kerugian global akibat kejahatan siber diperkirakan mencapai 10,5 triliun pada tahun 2025, meningkat signifikan dibandingkan 3 triliun pada tahun 2015 [1]. Di Indonesia, Badan Siber dan Sandi Negara (BSSN) mencatat terdapat lebih dari 361 juta anomali lalu lintas jaringan atau potensi serangan siber di Indonesia sepanjang Januari hingga Oktober 2023 [2], menandakan bahwa perusahaan di berbagai sektor semakin rentan terhadap ancaman siber.

PT Defender Nusa Semesta telah mengimplementasikan *Security Information and Event Management* (SIEM) sebagai bagian dari strategi pemantauan keamanan. Namun, tantangan utama yang dihadapi adalah tingginya jumlah *false positives*, di mana sistem sering mengidentifikasi aktivitas yang sebenarnya sah sebagai ancaman. SIEM menghasilkan ribuan hingga jutaan log harian, mayoritas bukan ancaman. Jika dianalisis secara manual, tim keamanan dapat mengalami *alert fatigue*, yang berisiko menyebabkan ancaman sebenarnya terabaikan.

Untuk mengatasi tantangan ini, perusahaan menerapkan strategi pemfilteran *alert* berbasis korelasi. Sistem hanya mengirim notifikasi untuk *valid threat* serta aktivitas mencurigakan yang perlu dikonfirmasi keabsahannya. Bahkan, SIEM juga bisa mengirimkan alarm yang salah, sehingga tim keamanan harus memilah ulang kembali agar hanya ancaman yang benar-benar valid yang ditindaklanjuti. Dengan pendekatan ini, perusahaan dapat lebih fokus dalam menangani insiden yang benar-benar berpotensi berbahaya, sehingga meningkatkan efisiensi dalam *incident response*.

Selain itu, serangan siber tidak memiliki pola waktu yang tetap dan dapat terjadi kapan saja, termasuk di luar jam kerja. Tanpa pemantauan yang berjalan selama 24 jam, serangan dapat berkembang tanpa terdeteksi hingga menyebabkan kerugian besar, seperti pencurian data atau sabotase sistem. Oleh karena itu,

penerapan strategi *security monitoring* yang efektif menjadi kebutuhan utama bagi perusahaan.

Dengan adanya sistem pemantauan yang berjalan selama 24 jam, perusahaan dapat mendeteksi anomali lebih cepat dan mengambil tindakan sebelum ancaman berkembang menjadi insiden yang lebih besar. Selain itu, strategi *incident response* yang sistematis memastikan bahwa setiap insiden yang terjadi dapat ditangani dengan prosedur yang jelas dan terstruktur, sehingga risiko dan dampak terhadap bisnis dapat diminimalkan. Dengan implementasi *security monitoring* yang optimal, perusahaan tidak hanya meningkatkan keamanan sistem tetapi juga memastikan kepatuhan terhadap regulasi keamanan siber yang berlaku.

1.2 Maksud dan Tujuan Kerja Magang

Tujuan dari pelaksanaan kerja magang di PT Defender Nusa Semesta adalah melakukan pemantauan dan analisis *event log* pada sistem keamanan informasi, mengidentifikasi potensi ancaman, serta memahami prosedur penanganan insiden yang diterapkan di lingkungan *Security Operations Center* (SOC). Selain itu, tujuan lainnya meliputi penerapan strategi monitoring yang sesuai standar operasional, pemanfaatan alat bantu keamanan (*security tools*), dan peningkatan pemahaman terhadap proses validasi, notifikasi, serta eskalasi insiden untuk memperkuat ketahanan siber perusahaan.

Secara spesifik, manfaat dari magang ini meliputi:

1. Meningkatkan keterampilan teknis dalam analisis log (*log analysis*), serta penggunaan berbagai *security tools* untuk mengidentifikasi dan merespons ancaman siber secara efektif.
2. Memperdalam pemahaman tentang strategi dan alur kerja *security monitoring* dan *incident response* melalui keterlibatan langsung dalam aktivitas operasional di lingkungan kerja *SOC*.
3. Mengembangkan kemampuan analisis, evaluasi risiko, serta pengambilan keputusan yang cepat dan tepat dalam menangani insiden keamanan, sesuai dengan standar dan prosedur operasional perusahaan.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Program magang di PT Defender Nusa Semesta berlangsung selama satu tahun, dimulai pada 3 Februari 2025 hingga 2 Februari 2026, dengan posisi sebagai *security analyst intern*. Program ini dilaksanakan selama empat hari dalam seminggu menggunakan sistem shifting, dengan total waktu kerja 40 jam per minggu. Lokasi PT Defender Nusa Semesta berada di Graha BIP lantai 6, Jalan Gatot Subroto, Jakarta Selatan, tempat seluruh operasional *Security Operations Center* (SOC) berlangsung.

Untuk memastikan pemantauan keamanan selama 24 jam, sistem kerja magang dibagi menjadi dua kelompok, yaitu Sayap Kiri (Minggu–Rabu) dan Sayap Kanan (Rabu–Sabtu). Hari Rabu seluruh tim SOC berkumpul dalam *weekly meeting* guna membahas evaluasi dan pembaruan mingguan. Selain itu, terdapat tiga jenis shift kerja, yaitu *early shift*, *mid shift*, dan *late shift*. Pembagian shift ini bertujuan untuk memastikan operasional SOC berjalan secara berkelanjutan dalam mendeteksi dan merespons insiden keamanan secara *real-time*. Tugas operasional SOC mulai dijalankan berdasarkan sistem shift yang telah ditentukan, dengan sistem kerja secara *work from office* (WFO).