BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam era digital yang semakin berkembang, keamanan data menjadi aspek krusial dalam kehidupan sehari-hari. Dengan meningkatnya ketergantungan pada teknologi digital, tantangan dalam melindungi data pribadi dan informasi sensitif pun semakin besar. Meskipun berbagai kemajuan telah dicapai dalam bidang keamanan data, tantangan seperti kualitas data, ketersediaan sumber daya komputasi, serta ancaman serangan *cyber* tetap menjadi perhatian utama yang perlu diselesaikan di masa depan [1]. Oleh karena itu, meningkatkan kesadaran akan pentingnya keamanan data menjadi langkah awal yang sangat penting dalam menghadapi *cyber threat* yang terus berkembang.

Kesadaran akan *cybersecurity (security awareness)* merupakan faktor utama dalam melindungi individu dan organisasi dari ancaman digital. Namun, penelitian menunjukkan bahwa tingkat *security awareness* masih belum optimal di berbagai kalangan, termasuk di lingkungan akademik. Tidak ada korelasi signifikan antara latar belakang pendidikan dan tingkat kesadaran *cybersecurity*, sehingga pelatihan keamanan yang komprehensif diperlukan bagi semua pengguna internet, terlepas dari latar belakang mereka [2]. Dengan meningkatnya *cyber threat* yang semakin canggih, diperlukan upaya edukasi yang lebih luas guna membentuk budaya *cybersecurity* yang lebih baik.

Cybersecurity adalah praktik perlindungan sistem komputer, jaringan, dan data dari serangan siber yang dapat mengancam kerahasiaan, integritas, dan ketersediaan informasi. Perlindungan ini menjadi sangat penting, mengingat ketergantungan individu maupun organisasi terhadap teknologi digital yang semakin tinggi [3]. Di berbagai sektor, mulai dari bisnis hingga pemerintahan, *cybersecurity* telah menjadi aspek fundamental dalam menjaga stabilitas dan keberlanjutan operasional. Namun, tantangan dalam *cybersecurity* tidak hanya terletak pada aspek teknis, tetapi juga pada kurangnya standar yang jelas dalam terminologi dan definisi di bidang ini, yang menghambat komunikasi dan perbandingan antarorganisasi dalam operasional keamanan [4]. Ditambah, masih terdapat tantangan dalam penerapan langkah-langkah keamanan yang efektif, terutama dalam hal bagaimana organisasi belajar dari insiden yang terjadi. Banyak

pendekatan keamanan saat ini lebih menitikberatkan pada investigasi pasca-insiden tanpa adanya model yang konsisten untuk mengimplementasikan pembelajaran dari insiden tersebut, sehingga meningkatkan risiko terulangnya ancaman yang sama di masa depan [5].

Salah satu pendekatan utama dalam *cybersecurity* adalah implementasi teknologi keamanan yang efektif. Namun, tantangan besar dalam penerapan teknologi *cybersecurity* di era Industri 4.0 adalah kurangnya solusi yang mempertimbangkan tiga lapisan utama dari sistem siber-fisik, yaitu fisik, jaringan, dan komputasi. Banyak solusi keamanan yang ada hanya berfokus pada aspek teknologi informasi tanpa mempertimbangkan strategi manajemen yang lebih holistik [6]. Oleh karena itu, pendekatan *cybersecurity* yang komprehensif harus mencakup teknologi mutakhir serta strategi yang mempertimbangkan berbagai aspek operasional dan manajerial.

Dalam dunia *cybersecurity*, konsep *red team* dan *blue team* menjadi strategi utama dalam menguji dan mempertahankan keamanan sistem. *Red team* bertugas melakukan simulasi serangan terhadap sistem dengan tujuan mengidentifikasi celah keamanan dan mengevaluasi sejauh mana sistem dapat bertahan dari ancaman eksternal. *Red teaming* sering kali diibaratkan sebagai ”penyerang” yang mencoba mengeksploitasi kelemahan dalam infrastruktur keamanan organisasi untuk meningkatkan kesiapan terhadap ancaman nyata [3].

Di sisi lain, *blue team* bertanggung jawab dalam mempertahankan sistem dan menanggulangi ancaman yang telah terdeteksi. *Blue team* bekerja dengan pendekatan defensif, yang mencakup pemantauan sistem, analisis ancaman, serta penerapan langkah-langkah mitigasi untuk melindungi sistem dari serangan. *Blue teaming* juga menggunakan kerangka kerja keamanan seperti MITRE ATT&CK, yang membantu dalam memahami pola serangan dan menyusun strategi pertahanan yang lebih efektif [7]. Dengan kombinasi teknik deteksi dan respons yang proaktif, *blue team* berperan penting dalam menjaga stabilitas dan keamanan sistem secara berkelanjutan.

Red teaming dan *blue teaming* sering kali bekerja secara terintegrasi di dalam *Security Operations Center (SOC)*, sebuah pusat operasi keamanan yang berfungsi untuk memonitor, mendeteksi, dan merespons insiden *cybersecurity* secara *real-time*. SOC dirancang untuk beradaptasi dengan ancaman yang berkembang, memastikan bahwa sistem keamanan organisasi selalu berada dalam kondisi optimal untuk menangkal serangan siber [4]. Sebagai bagian dari SOC, *security analyst* memainkan peran kunci dalam menganalisis ancaman, mengelola

insiden keamanan, dan mengembangkan strategi pertahanan yang lebih tangguh. Dengan meningkatnya kompleksitas serangan siber, peran *security analyst* menjadi semakin penting dalam menjaga keberlanjutan dan efektivitas keamanan sistem.

Sebagai upaya untuk menghadapi tantangan *cybersecurity* yang semakin kompleks, PT Defender Nusa Semesta (DNS) berkomitmen untuk menyediakan solusi keamanan yang inovatif dan andal melalui pengembangan sumber daya manusia yang kompeten di bidang *security monitoring* dan incident response. Program magang di DNS dirancang untuk memberikan pengalaman langsung kepada peserta dalam mengoperasikan sistem pemantauan keamanan serta menganalisis insiden siber secara *real-time*. Dengan pendekatan berbasis praktik dan supervisi dari para profesional, program ini bertujuan untuk membentuk tenaga ahli yang mampu menghadapi *cyber threat* di berbagai lingkungan bisnis dan industri. Sejalan dengan visi DNS sebagai mitra keamanan yang terpercaya, program ini juga mendukung misi perusahaan dalam meningkatkan standar keamanan informasi dengan memastikan bahwa setiap insiden dapat dideteksi, dianalisis, dan ditangani secara efektif guna menjaga integritas serta keberlanjutan sistem teknologi informasi. Hal ini menjadi penting karena tidak semua *alert* atau *alarm* yang muncul dalam sistem *monitoring* merupakan insiden yang valid, banyak di antaranya adalah *false positive* yang memerlukan analisis lebih lanjut untuk memastikan keabsahannya.

1.2 Maksud dan Tujuan Kerja Magang

Maksud dari program magang ini adalah untuk mengimplementasikan *security monitoring* serta *incident handling* dalam operasional SOC di PT Defender Nusa Semesta melalui pemantauan dan analisis terhadap *event log* yang masuk ke dalam sistem *security monitoring* Defenxor. Dalam pelaksanaannya, analisis dilakukan dengan menerapkan konsep-konsep *cybersecurity* yang telah dipelajari selama studi di Universitas Multimedia Nusantara, sehingga dapat mengembangkan keterampilan teknis dan praktis dalam mendeteksi serta merespons *cyber threat* secara efektif. Pengalaman langsung dalam pemantauan keamanan sistem memungkinkan pemahaman yang lebih mendalam mengenai pola insiden keamanan serta strategi mitigasi yang efektif untuk mencegah dampak yang lebih luas.

Selain menjadi bagian dari upaya peningkatan kapabilitas operasional SOC, program ini juga bertujuan untuk membentuk tenaga profesional yang kompeten

di bidang *cybersecurity* dengan pengalaman langsung dalam *security monitoring* dan *incident response*, guna menghadapi tantangan keamanan informasi yang terus berkembang. Implementasi yang dilakukan diharapkan dapat meningkatkan efektivitas operasional SOC dengan memastikan langkah-langkah deteksi dan respons terhadap *cyber threat* berjalan secara optimal. Dengan demikian, program ini berperan dalam mendukung pencapaian standar keamanan yang lebih tinggi serta memastikan sistem tetap terlindungi dari potensi risiko keamanan yang terus berkembang.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

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

Dalam program ini, terdapat sistem pembagian waktu kerja yang disebut sebagai sistem sayap, yang terbagi menjadi dua kelompok. Sayap kiri bekerja mulai dari hari Minggu hingga Rabu, sedangkan sayap kanan bekerja dari hari Rabu hingga Sabtu. Hari Rabu menjadi hari penting dalam sistem kerja ini, karena seluruh tim SOC berkumpul untuk mengikuti *weekly meeting* yang membahas evaluasi dan *update* mingguan. Selain itu, sistem kerja menggunakan metode *shifting* yang terdiri dari tiga jadwal, yaitu *early shift*, *mid shift*, dan *night shift*. Pembagian shift ini bertujuan untuk memastikan operasional SOC berjalan selama 24 jam dalam monitoring dan merespons insiden keamanan secara *real-time*.

Proses magang di PT Defender Nusa Semesta diawali dengan *training* selama satu bulan pertama, yang dirancang sebagai pembekalan pemahaman dasar sebelum terlibat langsung dalam kegiatan SOC. Materi *training* mencakup materi dasar *cybersecurity* dari Security+, serta latihan *case analysis* guna melatih keterampilan deteksi dan respons terhadap *cyber threat*. Setelah *training*, akan dimulai tugas operasional secara langsung di SOC dengan sistem *shifting* secara *work from office*. *Security monitoring* dilakukan berdasarkan waktu shift yang telah ditentukan oleh *team leader*, memastikan bahwa setiap bagian dari sistem *security monitoring* dapat beroperasi dengan optimal.

Tim SOC di PT Defender Nusa Semesta dipimpin oleh Bapak Andi

Wahyudi sebagai *Team Leader SOC Operation*, yang juga menjadi supervisor dalam program magang ini. *Team leader* bertanggung jawab dalam mengatur strategi operasional, mengoordinasikan tim dalam merespons insiden keamanan, serta memastikan efektivitas sistem pemantauan yang diterapkan. Sebagai bagian dari tim SOC, selama program magang, terdapat kesempatan untuk berkomunikasi dan berkoordinasi dengan berbagai anggota tim keamanan lainnya, termasuk *senior security analyst*, *engineer*, dan *sysadmin*.

Dalam program magang ini, terdapat sistem *buddy*, di mana *senior security analyst* bertugas untuk membantu dan membimbing berjalannya keseharian kerja magang. *Buddy* akan menjadi kontak pertama yang dihubungi saat ada hal-hal yang ingin ditanyakan selama proses kerja. Oleh karena itu, alur dari komunikasi kontak kerja harus melewati *buddy* dahulu, lalu *team leader*.