BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan komputer pada era digital semakin menghadapi tantangan besar. Serangan siber yang semakin canggih, seperti ransomware, malware, dan serangan phising, terus meningkat seiring pesatnya perkembangan teknologi. [1] Perkembangan teknologi tersebut beberapa diantaranya adalah berkembangnya *Internet of Things* (IoT), *cloud computing*, dan perangkat mobile, maka potensi vektor serangan yang dapat dieksploitasi pun kian meluas. [1] Namun, meskipun ancaman ini nyata, banyak organisasi yang masih kurang memperhatikan keamanan secara menyeluruh, terutama dalam hal memantau dan mendeteksi ancaman secara real-time.

Seiring dengan semakin kompleksnya lingkungan bisnis dan peningkatan risiko yang dihadapi oleh organisasi, pengendalian internal yang kuat menjadi semakin krusial. Teknologi, sebagai pendorong utama transformasi bisnis, menawarkan berbagai alat dan solusi untuk memperkuat pengendalian internal ini. [2]

Visibilitas terhadap potensi ancaman seringkali menjadi masalah utama. Banyak sistem keamanan komputer tidak memiliki kemampuan untuk mendeteksi ancaman dengan cepat atau merespon insiden secara efisien. Hal ini sering disebabkan oleh keterbatasan alat yang digunakan atau tidak adanya integrasi yang baik antar sistem keamanan. Organisasi kerap kali hanya fokus pada pencegahan serangan namun melupakan pentingnya monitoring yang aktif dan berkelanjutan. Kondisi ini membuat banyak perusahaan rentan terhadap serangan yang mungkin tidak terdeteksi selama berminggu-minggu atau bahkan berbulan-bulan. [3]

Untuk mengatasi masalah ini, penggunaan solusi keamanan yang lebih komprehensif menjadi semakin penting. Maka dari itu, peran Wazuh sebagai platform *Security Events* bisa dijadikan solusi. Wazuh merupakan Security Information and Event Management (SIEM) yang tidak hanya menawarkan deteksi ancaman secara real-time, namun juga memungkinkan pemantauan sistem secara menyeluruh. Dengan kemampuan integrasi yang luas dan monitoring endpoint yang detail, Wazuh membantu organisasi untuk meningkatkan visibilitas terhadap ancaman, mempercepat deteksi insiden, dan memberikan wawasan yang lebih

mendalam terkait keamanan jaringan. [4] Dengan menggunakan Wazuh, organisasi dapat mengadopsi pendekatan yang lebih proaktif dalam menjaga keamanan sistem mereka. Sebagai solusi open-source, Wazuh juga menawarkan fleksibilitas tinggi, mudah diintegrasikan dengan infrastruktur yang ada, serta didukung oleh komunitas global yang aktif dalam mengembangkan dan memperbarui fitur-fiturnya. [5]

Fungsi Wazuh dimaksimalkan dalam implementasi Wazuh SIEM di PT Global Innovation Technology, fokus utama dalam implementasi ini adalah integrasi *use case Security* dan pembuatan *dashboard* yang bertujuan untuk mengamankan *endpoint* dan mengumpulkan data tentang *Security Events* dengan menyesuaikan kebutuhan PT Global Innovation Technology dan mengamati kebutuhan *customer*.

1.2 Maksud dan Tujuan Kerja Magang

Berikut merupakan maksud dan tujuan pelaksanaan magang di PT Global Innovation Technology.

1.2.1 Maksud

1. Sebagai salah satu persyaratan kurikulum dan menambah wawasan di lingkungan kerja secara nyata di PT Global Innovation Technology.
2. Pendalaman materi terkait *Computer Security* yang sudah dipelajari pada perkuliahan.
3. Melakukan eksplorasi dengan tujuan mendalami tentang perangkat *monitoring* keamanan siber yang bernama Wazuh.

1.2.2 Tujuan

1. Melakukan implementasi Wazuh SIEM *Monitoring Tools* untuk membantu mengamankan *endpoint* IT yang dimiliki PT GIT.
2. Memperkenalkan produk Wazuh SIEM kepada klien selaku PT Global Innovation Technology adalah vendor penyedia pelayanan IT.
3. Membantu PT Global Innovation Technology mencari *use case* yang terkait dengan penggunaan Wazuh dengan sumber daya yang ada.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Pelaksanaan magang dilakukan berdasarkan kontrak kerja yang telah disetujui dan ditanda tangani dengan ketentuan 5 Hari kerja Senin - Jumat. Jam kerja dimulai dari pukul 08.00 WIB dan melakukan absensi masuk melalui aplikasi kantor yang bernama KejarTugas. Pukul 17.30 - 18.00 WIB merupakan jam pulang kerja dan akan melakukan absensi keluar melalui aplikasi.