BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital saat ini berlangsung sangat cepat dan memberikan banyak perubahan di berbagai bidang kehidupan. Hampir seluruh aktivitas, baik dalam dunia pendidikan, bisnis, maupun pemerintahan, kini bergantung pada sistem informasi berbasis internet. Namun, semakin canggih teknologi yang digunakan, semakin besar pula ancaman terhadap keamanan data dan sistem informasi. Berbagai serangan siber seperti pencurian data, peretasan situs web, serangan DDoS, hingga penyebaran malware menjadi tantangan serius yang harus dihadapi oleh organisasi maupun individu.

Keamanan siber *(cyber security)* menjadi aspek yang sangat penting untuk dipahami dan diterapkan, terutama oleh mereka yang bekerja di bidang teknologi informasi. Untuk menjaga keamanan sistem, dibutuhkan kombinasi antara perlindungan aplikasi berbasis internet dan aset fisik berupa perangkat keras. salah satu bentuk perlindungan yang digunakan adalah Cloudflare untuk keamanan aplikasi web, serta CrowdStrike Falcon sebagai solusi *endpoint security* untuk melindungi perangkat seperti laptop, PC, dan server dari malware maupun ancaman berbasis *file* mencurigakan.

Sayangnya, masih banyak organisasi yang belum memahami bagaimana proses analisis, pembuatan aturan *(rules)*, hingga pengambilan tindakan yang tepat dalam menangani serangan siber. Hal ini membuat sistem yang mereka gunakan berisiko mengalami kebocoran data atau kerusakan operasional. Oleh karena itu, dibutuhkan pemahaman yang baik mengenai bagaimana melakukan identifikasi, pembuatan *policy*, dan penerapan sistem keamanan yang sesuai untuk meningkatkan perlindungan aset digital maupun fisik.

Selama menjalani program magang pekerjaan di bidang keamanan siber, penulis berfokus pada penerapan sistem perlindungan aplikasi web menggunakan Cloudflare serta manajemen keamanan endpoint dengan CrowdStrike Falcon. Tujuan dari pekerjaan ini adalah untuk memahami proses analisis ancaman, pembuatan *rules* keamanan, dan penerapan kebijakan yang efektif sebagai upaya meningkatkan keamanan pada web aplikasi serta aset fisik organisasi.

1.2 Deskripsi Pekerjaan

It *security* melakukan tugas pengamanan pada aset digital perusahan baik dari aset tidak fisik maupun aset fisik. Dalam hal ini alat yang digunakan pada kegiatan kerja yang berhubungan dengan internet contoh laptop, pc dan server. Pekerjaan ini mendapat kepercayaan dari perusahan untuk memegang kendari terhadap keamanan aset.

Dalam menjalan tugas pengaman aset it security mendapatkan akses ke *endpoint security* yaitu falcon crowdstrike yang berguna sebagai anti virus dengan agent yang tertanam langsung pada divais setiap karyawan perusahan.

Pada aset digital dalam melakukan pengamanan menggunakan web aplikasi *security* cloudflare yang bekerja sebagai firewall penggunaan cloudflare it security berfokus pada penggunaan role untuk membatasi akses pengguna ke *path* yang tidak boleh diakses oleh *end user*.

1.3 Tujuan

Dalam magang ini bertujuan untuk melakukan uji coba pengamanan aset digital maupun fisik yang dilakukan menggunakan cloudflare untuk aset digital dan crowdstrike falcon digunakan untuk aset fisik:laptop, pc dan server.layanan ke

1.4 Manfaat

Penggunaan cloudflare untuk melakukan pengamanan pada aset digital (web aplikasi) dengan menggunakan roles yang ada pada cloudflare, memahami penggunaan fitur http *traffic* untuk melakukan pengamatan pada long yang ada pada web aplikasi untuk mempermudah melakukan pengamatan dan menentukan

waf yang akan digunakan pada http *traffic* terdapat parameter quest dari berbagai negara untuk melihat akses dari negara mana yang paling sering terjadi selain dari negara utama web app tersebut digunakan

Penggunaan crowdstrike falcon dalam melakukan pengamanan aset fisik menggunakan endpoint detections yang bergunan untuk melihat secara detail long deteksi atau indikasi virus yang ada pada host (pc,laptop, server yang install *agent*) dengan fitur ini penulis menggunakan endpoint ini untuk melihat detail apa indikasi virus tersebut beresiko dan harus diambil tindakan melakukan pengurugan pada *file* indikasi virus dan ambil tindakan pada *file* tersebut.