BAB II
PROFIL INSTANSI TEMPAT MAGANG

2.1 Manfaat

Lingkup pada organisasi mitra berfokus pada layanan streaming video secara online berbayar pada program magang penulis berfokus pada pengaman aset digital dan aset penunjang kelancaran organisasi dalam menjalankan usaha penulis berperan dalam pengamanan aset digital dan nondigital yang ada pada perusahaan penerapan yang dilakukan pada aset digital seperti web app dilakukan dengan pengaman pada WAF yang lebih berfokus pada pembatasan akses pada *path* tertentu dan *rules* yang bertujuan untuk pengamanan pada web app, melakukan pentest internal untuk mengetahui pada sistem web app terdapat kerentanan yang dapat mengganggu jalannya usaha.

2.2 Struktur Organisasi

Gambar 2.1. Struktur Organisasi

1. **Komisaris (Nezim)**

   Berikut ini merupakan tugas dari komisaris:

   a. Memberikan instruksi kepada seluruh divisi yang ada pada perusahaan agar berjalan sesuai dengan visi dan misi perusahaan.
   b. Memastikan Keputusan direksi sejalan dengan kepentingan perusahaan dan pemegang saham.
   c. Melakukan penilaian terhadap kinerja direksi.

2. **Direktur (Andrean Aradyka)**

   Berikut ini merupakan tugas direktur:

   a. Memberi Keputusan pada strategi yang akan diambil oleh perusahaan.
   b. Memimpin dan mengelola operasional perusahaan.
   c. Memegang kendali tertinggi Perusahaan.

3. **VP Business (Heril Juliawan AS)**

   Berikut ini merupakan tugas dari VP business:

   a. Mengembangkan rencana mitigasi risiko untuk menjaga stabilitas Perusahaan
   b. Membangun dan memelihara hubungan dengan mitra strategis, pelanggan utama, dan investor
   c. Memastikan bahwa target pendapatan perusahaan tercapai

4. **Security Manager SOC & Blue Team (Sulhaedir)**

   Berikut ini merupakan tugas security manager soc manager soc & blue team:

   a. Membimbing tim Blue Team dalam mengidentifikasi, menganalisis, dan memperbaiki kelemahan keamanan.
   b. Melakukan pengecekan terhadap laporan dari L1 dan melakukan validasi untuk dibuat laporan kepada pihak klien.
   c. Melakukan laporan bulan kepada klien.

5. **SOC Analyst (Andri Dwi, Aditya M)**

   Berikut ini merupakan tugas dari soc analyst:

   a. Membantu mitigasi ancaman
   b. Mengidentifikasi aktivitas mencurigakan atau anomali yang berpotensi menjadi ancaman keamanan.
   c. Memberikan rekomendasi langkah mitigasi untuk mengurangi resiko serangan berulang.

6. **Legal (Bintang Mandhala)**

   Berikut ini merupakan tugas dari legal:

   a. Memastikan bahwa semua aktivitas perusahaan sesuai dengan peraturan perundang-undangan yang berlaku baik secara lokal maupun internasional
   b. Menyusun, memeriksa, dan merevisi perjanjian atau kontrak kerja sama baik dengan mitra bisnis,vendor, maupun pihak ketiga lainnya.
   c. Memberikan nasihat hukum untuk perusahaan.

7. **Security Engineer Red Team & Digital Forensic (Dwi Andi S)**

   Berikut ini merupakan tugas dari security engineer red team & digital forensic:

   a. Mengembangkan sistem keamanan Perusahaan.
   b. Memimpin red team dalam melakukan pengujian pada sistem keamanan dengan melakukan simulasi serangan
   c. Memberikan saran teknik kepada blue team dalam membuat sistem keamanan

8. **Red Team (Rahmat Ramadhan, Ari Apridana):**

   Berikut ini merupakan tugas dari red team:

   a. Melakukan simulasi serangan untuk mengidentifikasi kerentanan dalam sistem.

b. Menganalisa hasil eksploitasi untuk memberikan wawasan tentang potensi dan resiko keamanan pada system.
c. Melakukan berbagai simulasi serangan untuk menguji sistem keamanan.

9. Security Compliance (Priyanka Ayu)

Berikut ini merupakan tugas dari security compliance:

a. Memastikan perusahaan mematuhi regulasi seperti GDPR, ISO27001, PCI-DSS, HIPAA, atau standar keamanan lainnya yang relevan atau local.
b. Memastikan bahwa kontrol keamanan diterapkan secara konsisten di seluruh Perusahaan.
c. Berperan dalam proses audit dengan penyedia layanan pihak ketiga.

2.3 Lingkup Pekerjaan

1. Memantau Keamanan Sistem

   Secara aktif mengawasi aktivitas jaringan dan sistem melalui alat pemantauan (monitoring tools) untuk mendeteksi aktivitas mencurigakan atau ancaman keamanan.
2. Menganalisis dan Menindaklanjuti Peringatan (Alerts)

   Memeriksa peringatan yang muncul dari sistem keamanan, seperti firewall atau antivirus, untuk menentukan apakah peringatan tersebut benar-benar ancaman atau hanya kesalahan (false positive).
3. Mencatat dan Melakukan respon pada Peringatan (Alert)

   Melakukan penanganan pada peringatan yang muncul dengan melakukan pengecekan apakah itu merupakan serangan.
4. Melakukan pengambilan tindakan

   Mengambil tidak dengan melakukan penetapan role baru pada

system atau melakukan pemberitahuan untuk melakukan update pada system ke aman.

5. Berkomunikasi dengan Tim Lain
   Berkolaborasi dengan tim IT atau SOC Level 2 untuk memastikan ancaman yang lebih kompleks dapat ditangani dengan cepat dan tepat.
6. Mengevaluasi dan Mengupdate Prosedur Keamanan
   Membantu memperbarui kebijakan dan prosedur keamanan berdasarkan ancaman terbaru yang ditemukan selama pemantauan.

2.4 Deskripsi Pekerjaan

Melakukan monitoring harian pada aset digital dan nondigital pada perusahan menggunakan *dashboard* monitoring long bawan dari crowdstrike dan cloudflare kedua *dashboard* tersebut diakses secara online web *dashboard* pada *dashboard* penulis bertugas untuk melakukan pemantauan pada long masuk pada kedua dashboard dan membuat roles atau policy saat dibutuhkan pengambilan tindakan dan melakukan konfirmasi terlebih dahulu pada SOC manager untuk dilakukan penyesuaian terhadap *roles* atau *policy* yang dibuat sudah sesuai dan tidak mengganggu jalan operasi web aplikasi atau pc,laptop dan server yang digunakan.

Scan report selain melakukan pemantauan *dashboard* dan pembuatan *rules* dan *policy* penulis bertugas untuk melakukan va scan secara rutin terhadap semua aset digital dalam hal ini adalah aset web aplikasi yang dimiliki perusahan hal ini dilakukan untuk memastikan semua aset web aplikasi tidak menggunakan versi servis yang terdapat kerentan di dalamnya hal ini dilakukan secara rutin setiap dua minggu sekali.

2.5 Jadwal Kerja

Tabel 2.1. Jadwal Kegiatan Magang

Waktu	Kegiatan
Minggu 1 & 2 (Maret tanggal 1-15)	1. Memulai pentest (uji penetrasi) web apk xxxx. 2. Pembuatan laporan awal di Jira. 3. Instalasi/pemasangan lisensi tool untuk pentest. 4. Monitoring CrowdStrike dan Cloudflare.
Minggu 3 & 4 (Maret tanggal 15-31)	1. Perluasan cakupan pentest xxxxxx ke platform mobile 2. Pembuatan laporan di xxxxx 3. Penarikan laporan dari Cloudflare dan CrowdStrike. 4. Scan rutin per dua minggu pada aset xxxx dengan Nessus
minggu 1&2 (April tanggal 1-15)	1. Melanjutkan pentest dari bulan maret minggu ke 4 (W4) 2. pembuatan laporan rutin dua mingguan di xxx 3. pemantauan rutin harian cloudflare dan crowdstrike 4. scan rutin per 2 minggu pada aset dengan menggunakan nessus
Minggu 3&4 (April Tanggal 16-31)	1. Melanjutkan pentest dari bulan Maret minggu ke-4 (W4) 2. Pembuatan laporan rutin dua mingguan di Atlassian 3. Pemantauan rutin harian Cloudflare dan CrowdStrike 4. Scan rutin per dua minggu pada aset xxxx dengan Nessus

Minggu 1 & 2 (May 1-15)	1. Persiapan audit 2. Pemantauan rutin harian Cloudflare dan CrowdStrike. 3. Pembuatan laporan rutin dua mingguan di xxxx 4. Scan rutin pada aset xxxx dengan Nessus
Minggu 3 & 4 (May 16 -31)	1. Pelaksanaan audit 2. Penambahan cakupan pentest ke aset xxxxx. 3. Memulai tahapan scan pada aset xxxxxx 4. Scan rutin pada aset xxxx dan xxxxx dengan Nessus. 5. Instalasi Open CTI. 6. Pemantauan rutin Cloudflare dan CrowdStrike. 7. Pembuatan laporan rutin dua mingguan di xxxx.
Minggu 1 & 2 (Juni 1-15)	1. Memulai pentest pada aset Como dengan cakupan (xxxxxxxxxxx) 2. Scan rutin aset xxx dan no-xxx dengan Nessus. 3. Pembuatan laporan rutin dua mingguan pada xxx 4. Pemantauan rutin Cloudflare dan CrowdStrike.
Minggu 3 & 4 (juni 16-30)	1. Memulai penilaian antivirus baru poc. 2. Wireless scan (pemindaian nirkabel) pada jaringan xxx. 3. Pemantauan rutin Cloudflare dan

	CrowdStrike. 4. Pembuatan laporan rutin dua mingguan pada xxx