KERJA PRAKTIK - IF184801

Penggunaan Threat Map Pada PT PLN Nusantara Power Dalam Monitoring Analisa Keamanan Sistem Unit Pembangkit Listrik

PT. PLN Nusantara Power

Kantor Pusat Jl.Ketintang Baru no.11 Surabaya

Periode: 6 Januari 2025 - 5 April 2025

Oleh:
Schaquille Devlin Aristano 5025211211

Pembimbing Departemen
Prof. Dr. Diana Purwitasari, S.Kom., M.Sc.
Pembimbing Lapangan
Muhammad Sokheh, S.Kom

DEPARTEMEN TEKNIK INFORMATIKA
Fakultas Teknologi Elektro dan Informatika Cerdas Institut Teknologi Sepuluh Nopember
Surabaya 2025

KERJA PRAKTIK - IF184801

Penggunaan Threat Map Pada PT PLN Nusantara Power Dalam Monitoring Analisa Keamanan Sistem Unit Pembangkit Listrik

PT. PLN Nusantara Power
Kantor Pusat Jl.Ketintang Baru no.11 Surabaya
Periode: 6 Januari 2025 - 5 April 2025

Oleh:
Schaquille Devlin Aristano 5025211211

Pembimbing Departemen
Prof. Dr. Diana Purwitasari, S.Kom., M.Sc.
Pembimbing Lapangan
Muhammad Sokheh, S.Kom

DEPARTEMEN TEKNIK INFORMATIKA
Fakultas Teknologi Elektro dan Informatika Cerdas Institut Teknologi Sepuluh Nopember
Surabaya 2025

DAFTAR ISI

[Halaman ini sengaja dikosongkan]

DAFTAR GAMBAR

[Halaman ini sengaja dikosongkan]

DAFTAR TABEL

[Halaman ini sengaja dikosongkan]

DAFTAR KODE SUMBER

[Halaman ini sengaja dikosongkan]

LEMBAR PENGESAHAN

KERJA PRAKTIK

Penggunaan Threat Map Pada PT PLN Nusantara Power Dalam Monitoring Analisa Keamanan Sistem Unit Pembangkit Listrik

Oleh:

Schaquille Devlin Aristano 5025211211

Disetujui oleh Pembimbing Kerja Praktik:

1. Prof. Dr. Diana Purwitasari, S.Kom., M.Sc.
   197804102003122001

(Pembimbing Departemen)

1. Muhammad Sokheh , S.Kom.

(Pembimbing Lapangan)

[Halaman ini sengaja dikosongkan]

Penggunaan Threat Map Pada PT PLN Nusantara Power Dalam Monitoring Analisa Keamanan Sistem Unit Pembangkit Listrik

Nama Mahasiswa	:	Schaquille Devlin Aristano
NRP	:	5025211211
Departemen	:	Teknik Informatika FTEIC-ITS
Pembimbing Departemen	:	Prof. Dr. Diana Purwitasari, S.Kom., M.Sc.
Pembimbing Lapangan	:	Muhammad Sokheh, S.Kom.

ABSTRAK

Dengan meningkat banyaknya ancaman siber dalam beberapa dekade ini maka PT PLN Nusantara Power membutuhkan cara untuk menganalisis keamanan sistem. Oleh karena itu, dilakukan kerja praktek dengan tujuan untuk mengembangkan Threat Map.

Threat Map dikembangkan dengan javascript dan menggunakan library D3.js untuk memvisualisasikan data serangan dan leaflet.js untuk menampilkan peta interaktif. Dataset yang digunakan terdapat dari *random number generator* agar tidak menggunakan data yang sensitif dari PT PLN Nusantara Power.

Aplikasi yang dikembangkan menggunakan tools yang kurang familiar dan perencanaan yang kurang matang hingga menghasilkan aplikasi yang memiliki *user interface* kurang intuitif dengan fitur dan interaktivitas yang minimal.

Kata Kunci: Threat Map, Keamanan sistem, Javascript

[Halaman ini sengaja dikosongkan]

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT karena atas berkah dan rahmatNya penulis dapat menyelesaikan kerja praktik yang dilaksanakan di PT. PLN Nusantara Powers dan menyelesaikan laporan kerja praktik yang membahas materi Penggunaan Threat Map dalam menganalisa keamanan sistem unit-unit pembangkit listrik.

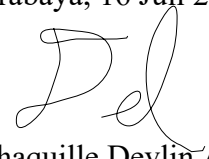
Adapun tujuan dari kerja praktik ini yaitu sebagai salah satu syarat untuk menyelesaikan mata kuliah Kerja Praktik (4 SKS) pada jurusan Teknik Informatika FTEIC ITS. Selain itu kegiatan ini juga bertujuan untuk meningkatkan pemahaman serta pengalaman penulis dalam aplikasi dari ilmu yang diajarkan di perkuliahan.

Dalam melaksanakan kerja praktik ini penulis banyak mendapatkan bantuan juga bimbingan, nasehat dan masukan yang sangat berguna dalam memahami materi dan permasalahan yang ada. Oleh karenanya pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Kedua orang tua penulis.
2. Bapak Ary Mazharuddin Shiddiqi S.Kom., M.Comp., Ph.D, 1. selaku koordinator Kerja Praktik.
3. Prof. Dr. Diana Purwitasari, S.Kom., M.Sc. selaku dosen pembimbing Kerja Praktik ini.
4. Bapak Harry Purnomo selaku Vice President Corporate Communication and CSR
5. Bapak Ir. Fatkul Mubin selaku Vice President Information Technology and Digital
6. Bapak Muhammad Sokheh, S.Kom selaku pembimbing utama kerja praktik

7. Bapak Ir. Bambang Prastyo Wibowo selaku pembimbing kerja prakek
8. Bapak Taufik Rachman selaku pembimbing kerja praktik

Surabaya, 16 Juli 2025



Schaquille Devlin Aristano

BAB I
PENDAHULUAN

1.1 Latar Belakang

Threat Map adalah aplikasi yang dapat memvisualisasikan serangan siber dalam waktu nyata atau serangan siber yang lalu pada sebuah jaringan, peralatan dan sistem komputer. Ini berfungsi untuk menganalisa ancaman siber dengan sumber data dan teknik visualisasi untuk menentukan pola dan kerentanan yang mungkin ada [1].

Seiring berkembangnya teknologi komputer, maka ketergantungan manusia terhadap komputer makin meningkat dan ini menarik perhatian penjahat siber yang ingin mengakses data-data yang sensitif dari berbagai badan dengan tujuan menuntut tebusan pihak bersangkutan. Dengan meningkat banyaknya ancaman siber selama beberapa dekade ini, maka perusahaan keamanan siber mengembangkan Threat Map sebagai alat untuk memonitorkan ancaman-ancaman siber [2]

PT PLN Nusantara Power sebelumnya dikenal sebagai PT PJB (Pembangkitan Jawa-Bali) adalah BUMN yang berdiri sejak tahun 1995 [3]. Pada kuartil ketiga tahun 2024, Indonesia menghadapi 800 juta serangan siber dengan pola yang semakin kompleks. Para pakar keamanan siber memprediksi bahwa pada

tahun 2025 akan ada sekitar 2 miliar serangan per tahun di Indonesia [4] dan sebagai BUMN, PT PLN Nusantara Power menjada sasaran kritis utama bagi para hacker. Maka begitu penting untuk memiliki keamanan sistem yang baik. Untuk memastikan keamanan sistem diharuskan memiliki cara untuk menganalisis ancaman sistem, dan PT PLN Nusantara Power mengatasinya dengan menggunakan Threat Map.

1.2 Tujuan

Tujuan dari kerja praktik ini adalah untuk menyelesaikan kewajiban mata kuliah kerja praktik pada departemen Teknik Informatika, Fakultas Teknik Elektro Dan Informatika Cerdas - Institut Teknologi Sepuluh Nopember dengan bobot 4 (empat) SKS. Selain itu, tujuan lainnya adalah untuk membantu PT PLN Nusantara Power dalam mengembangkan Threat map untuk memudahkan analisis keamanan sistem.

1.3 Manfaat

Manfaat yang dapat diperoleh dari kegiatan pengembangan applikasi Threat Map ini antara lain :

1. Penulis memahami threat map sebagai pengetahuan baru yang selama ini belum diperoleh dalam perkuliahan.
2. Penulis mampu membuat threat map hingga dapat menjalankan fungsi dasar dan akan terus berusaha mengembangkannya sehingga bisa menampilkan lebih banyak data.

3. Menginspirasi penulis untuk lebih mendalami berbagai aplikasi keamanan sistem.

1.4 Rumusan Masalah

Berikut ini rumusan masalah pada kerja praktik pengembangan threat map:

1. Bagaimana membuat sebuah Threat Map yang dapat memudahkan analisis keamanan sistem.
2. Bagaimana mengembangkan threat map yang ada agar lebih relevan untuk kebutuhan PT PLN NP

1.5 Lokasi dan Waktu Kerja Praktik

Kerja praktik ini dilaksanakan pada waktu dan tempat sebagai berikut:

Lokasi	: PT. PLN Nusantara Power
Alamat	: Jl.Ketintang Baru no.11 Surabaya 60231
Waktu	: 06 Januari 2025 - 05 April 2025
Hari Kerja	: Senin - Jumat
Jam Kerja	: 07.30 - 16.00

1.6 Metodologi Kerja Praktik

1.6.1 Perumusan Masalah

Untuk mengetahui spesifikasi fitur aplikasi threat map yang diinginkan oleh PT PLN Nusantara Power, pembimbing lapangan menbahas rincian kebutuhan aplikasi threat map yang akan dibangun. setelah dibahaskan, lalu dirumuskan fitur-fitur yang akan

diimplementasikan pada aplikasi threat map yang akan dibuat.

1.6.2 Studi Literatur

Setelah ditentukan kebutuhan aplikasi yang akan dibuat, dilakukan studi literatur mengenai cara mengimplementasinya. Pada tahap ini dilakukan pencarian dan pembelajaran informasi dari internet yang dapat membantu dalam merumuskan solusi dan implementasinya.

1.6.3 Solusi dan Implementasi Sistem

Tahap ini meliputi pengimplementasian aplikasi berdasarkan kebutuhan yang sudah ditentukan. Implementasi Threat Map menggunakan library D3 dan LeafletJS. Jika ada masukan dari pembimbing lapangan maka disertakan pada aplikasi segera mungkin.

1.6.4 Pengujian dan Evaluasi

Setelah aplikasi yang direncanakan sudah dibuat, dilakukan pengujian untuk menentukan apakah fitur-fitur aplikasi sudah sesuai dengan kebutuhan yang ditentukan. Kesesuaian aplikasi dengan kebutuhan menentukan keberhasilan dalam pengujian. Jika masih belum sesuai maka penulis kembali ke tahap Implementasi.

1.7 Sistematika Laporan

1.7.1 Bab I Pendahuluan

Pada bab ini dijelaskan tentang latar belakang permasalahan, tujuan kerja praktik, waktu pelaksanaan, serta sistematika pengerjaan kerja praktik dan juga penulisan laporan kerja praktik.

1.7.2 Bab II Profil Perusahaan

Pada bab ini dijelaskan secara rinci profil perusahaan tempat penulis melaksanakan kerja praktik yakni PT. PLN Nusantara Power pada bidang pengembangan teknologi industri.

1.7.3 Bab III Tinjauan Pustaka

Pada bab ini dijelaskan mengenai tinjauan pustaka dan literatur yang digunakan dalam menyelesaikan kerja praktik.

1.7.4 Bab IV Pengerjaan Kerja Praktik

Pada bab ini dijelaskan mengenai kegiatan yang dilakukan selama kerja praktik di PT PLN Nusantara Power pada bidang pengembangan teknologi industri.

1.7.5 Bab V Kesimpulan dan Saran

Pada bab ini berisi kesimpulan yang dapat diambil dan saran selama pengerjaan kerja praktik.

[Halaman ini sengaja dikosongkan]

BAB II
PROFIL PERUSAHAAN

2.1 Profil PT. PLN Nusantara Power

PT PLN Nusantara Power (PT PLN NP) sejak berdiri tahun 1995 yang awalnya bernama PT Pembangkitan Jawa-Bali (PT PJB) senantiasa mengabdikan diri untuk bangsa dan negara Indonesia, serta mendorong perkembangan perekonomian nasional dengan menyediakan energi listrik yang bermutu tinggi, andal dan ramah lingkungan. Dengan visi menjadi perusahaan pembangkit tenaga listrik Indonesia yang terkemuka dengan standar kelas dunia. PT PLN NP tiada henti berbenah dan melakukan inovasi dengan tetap berpegang pada kaidah tata pengelolaan perusahaan yang baik (Good Corporate Governance/GCG). Berkat dukungan shareholders dan stakeholders, PT PLN NP tumbuh dan berkembang dengan berbagai bidang usaha, tanpa meninggalkan tanggung jawab sosial perusahaan demi terwujudnya kemandirian masyarakat dan kelestarian lingkungan hidup.

2.2 Logo Perusahaan

Gambar 2.1 Logo PLN Nusantara Power

2.3 VISI dan MISI

2.3.1 VISI

- Menjadi perusahaan pembangkitan yang terdepan dan terpercaya untuk energi berkelanjutan di Indonesia dan pasar global

2.3.2 MISI

- Menjaga kinerja pembangkitan listrik yang unggul sebagai kompetensi inti
- Membangun bisnis inovatif yang terdepan untuk melakukan diversifikasi dan pertumbuhan yang berkelanjutan
- Mengakselerasi portofolio bisnis EBT untuk mendukung tercapainya nol emisi karbon
- Mengakuisisi dan membangun talenta terbaik untuk menjalankan organisasi yang responsif dan adaptif

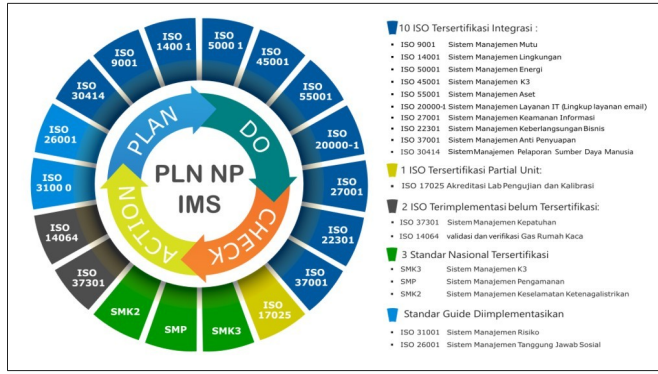
2.4 Solusi Bisnis PT PLN Nusantara Power

- Peningkatan kapasitas pembangkit
- Operation dan maintenance (O&M)
- Maintenance repair overhaul (MRO)
- Engineering procurement construction (EPC)
- Sparepart / material
- Power quality
- Green power
- Asset light

Gambar 2.2 Peta Operasional PT PLN NP

Peningkatan kapasitas pembangkit PLN NP dari 7,76 GW saat pra HSH menjadi 23,71 GW paska HSH sampai dengan tahun 2025.

2.5 Integrated Management System



Gambar 2.3 Sistem Manajemen Intergrasi

Terdapat 18 sistem manajemen yang telah diimplementasikan, dimana 14 sistem manajemen nasional dan internasional telah tersertifikasi, 2 sitem manajemen telah

diterapkan namun belum tersertifikasi, dan telah mengimplementasikan 2 standard guide.

Sistem manajemen tersebut antara lain :

1. Sistem manajemen mutu (ISO 9001:2015)
2. Sistem manajemen lingkungan (ISO 14001:2015)
3. Sistem manajemen energi (ISO 50001:2018)
4. Sistem manajemen K3 (ISO 4500:2018, SMK3)
5. Sistem manajemen keselamatan ketenagalistrikan (SMK2)
6. Sistem manajemen aset (ISO 55001:2014)
7. Sistem manajemen layanan teknologi informasi (ISO 20000-1:2018)
8. Sistem manajemen pengamanan informasi (ISO 27001:2013)
9. Sistem manajemen kesinambungan bisnis (ISO 22301:2019)
10. Sistem manajemen anti penyuapan (ISO 37001:2016)
11. Sistem manajemen pelaporan sumber daya manusia (ISO 30414:2018)
12. Sistem manajemen kepatuhan (ISO 37301:2021)
13. Sistem manajemen validasi dan verifikasi gas rumah kaca (ISO 14064:2018)
14. Standar akreditasi laboratorium pengujian dan kalibrasi (ISO 17025:2017)

Hal ini menjadikan PLN Nusantara Power senantiasa melaksanakan proses bisnisnya secara sitematik, terukur, dan selalu berupaya melakukan perbaikan berkelanjutan.

BAB III
TINJAUAN PUSTAKA

3.1 HTML

HTML atau Hypertext Markup Language adalah standard markup language yang digunakan untuk pemrograman web. Elemen HTML adalah dasar pembangun halaman HTML yang dapat mengandung gambar dan objek lainnya seperti form interaktif untuk dibenamkan pada halaman web. HTML umumnya digunakan bersama dengan CSS dan javascript untuk membuat halaman web yang dinamis [5].

3.2 Javascript

Javascript adalah bahasa programming *multi-paradigm high-level* ringan yang digunakan dalam pemrograman web. Umumnya Javascript digunakan untuk menambahkan interkasi dinamis pada halaman web, aplikasi, dan server. Javascript digunakan sebagai bahasa utama dalam pengembangan aplikasi Threat Map.

Awalnya hanya digunakan untuk pengunaan internal. Namun menjadi publik setelah Netscape mengajukannya pada ECMA Internasional sebagai spesifikasi standar untuk web browser. Javascript banyak digunakan oleh kerangka dan library seperti AngularJS, jQuery, ReactJS dan Node.js [6].

3.3 D3.js

D3.js (Data-Driven Document) adalah library Javascript untuk memvisualisasikan data secara dinamis dan interaktif pada halaman web yang mengikuti standar web seperti HTML, CSS dan SVG. D3.js dapat membuat graf yang unik dan berpenampilan seseuai kebutuhan pengguna. Penggunaan utama D3 daam aplikasi ini adalah untuk menggunakan fungsi untuk mengurai dataset dari file CSV.

D3.js bekerja dengan mengikat data ke DOM element dan menerapkan transformasi kepada elemen tersebut. Ini membiarkan visualisasi dinamis dan fleksibel yang dapat diperbarui seiring perubahan data [7].

3.4 Leaflet.js

Leaflet.js adalah library javascript open-source ringan untuk membuat peta interaktif dan menampilkan data peta. Peta terdiri lapisan *tile* bersama dengan *browser support, default interactivity,* kemampuan panning dan zooming. Leaflet.js dapat digunakan pada platform desktop dan mobile membuatnya cocok untuk perangkat smartphone [8] dan digunakan untuk menampilkan dan berinteraksi dengan peta dalam aplikasi.

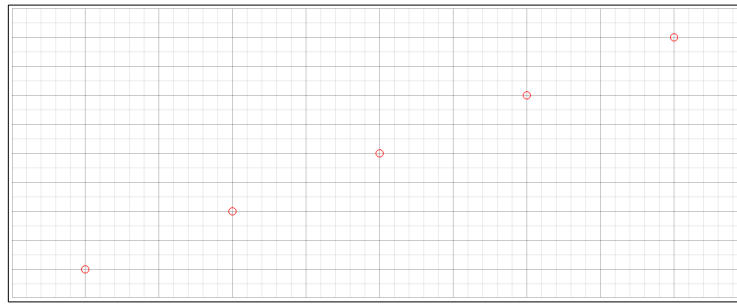
BAB IV
PENGERJAAN KERJA PRAKTEK

4.1 Analisis Kebutuhan Pengguna

Tahapan awal yang penulis lakukan dalam pembuatan aplikasi Threat Map adalah mempelajari tools yang dibutuhkan, karena perencanaan penggunaan tools adalah faktor penting dalam mengembangkan aplikasi.

Setelah mempelajari kebutuhan pengguna penulis mulai membuat Threat Map menggunakan tools yang tidak familiar yaitu Rust dan Plotter, dan hasilnya kurang bagus karena tidak ada interaktivitas dengan user dan terbatas dalam hanya memberikan output file PNG statik dimana adanya kebutuhan aplikasi Threat Map untuk bisa diintegrasikan ke sistem keamanan PLN Nusantara Power yang berbentuk web serta dapat berinteraksi dengan peta seperti melihat detil serangan atau unit yang diserang.

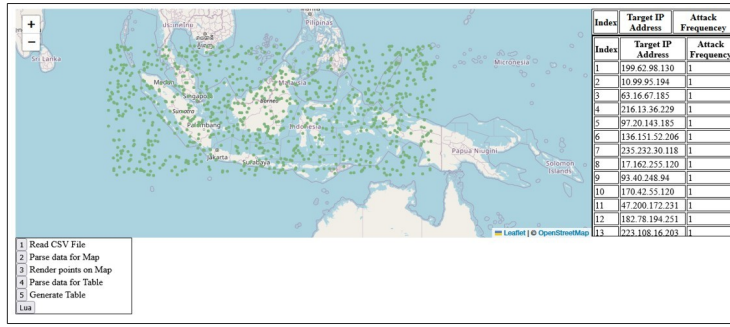
Berdasarkan analisa kebutuhan pengguna penulis harus menggantinya dengan tools yang lebih familiar agar Threat Map yang dihasilkan bisa mudah diintegrasi dengan web yang ada.



Gambar 4.1 Prototype aplikasi menggunakan Rust dan Plotter

4.2 Pengembangan Aplikasi

Langkah berikutnya yang penulis lakukan dalam pengembangan aplikasi Threat Map ini adalah menggunakan HTML, Javascript, D3 dan Leaflet



Index	Target IP Address	Attack Frequency
1	199.62.98.130	1
2	10.99.95.194	1
3	63.16.67.185	1
4	216.13.36.229	1
5	97.20.143.185	1
6	136.151.52.206	1
7	235.232.30.118	1
8	17.162.255.120	1
9	93.40.248.94	1
10	170.42.55.120	1
11	47.200.172.231	1
12	182.78.194.251	1
13	223.108.16.203	1

Gambar 4.2 Threat Map dengan menggunakan HTML, Javascript, D3 dan Leaflet

Threat Map yang dihasilkan dapat menjalankan fungsi dasar yang diminta oleh pembimbing yaitu dapat

memunculkan data-data yang dibutuhkan, tetapi karena keterbatasan waktu penulis belum dapat mengembangkan aplikasi sehingga dapat memunculkan lebih banyak lagi data yang dibutuhkan.

4.3 Penjelasan Kode

Pertama, semua *library* yang dibutuhkan untuk program perlu diimpor terlebih dahulu.

```
15  <script src="./script.js"></script>
16  <script src="./calc.js"></script>
17  <link rel="stylesheet" href="https://unpkg.com/leaflet@1.9.4/dist/
    leaflet.css" integrity="sha256-p4NxAoJBhIIN+hmNHrzRCf9tD/miZyoHS5o
    bTRR9BMY=" crossorigin=""/>
18  <script src="https://unpkg.com/leaflet@1.9.4/dist/leaflet.js"integrity=
    "sha256-20nQCchB9co0qIjJZRGuk2/Z9VM+kNiyxNV1lvTlZBo="crossorigin="">
    </script>
19  <script src="https://d3js.org/d3.v4.js"></script>
20  <script src="fengari-web.js" type="text/javascript" async></script>
21  <script src="https://cdnjs.cloudflare.com/ajax/libs/p5.js/0.5.16/
    p5.min.js" type="text/javascript"></script>
```

Kode Sumber 4.1 Impor library

4.3.1 Data Reader

Setelah *library* yang dibutuhkan sudah diimpor, file csv yang mengandung data akan dibaca menggunakan D3 dan dimasukkan ke dalam array

```
 1  async function read_file(filename)
 2  {
 3    let arr = [];
 4    d3.csv(filename, (d) => {
 5      for (let i = 0; i < d.length; i++)
 6      {
 7        arr.push(d[i]);
 8      }
 9    });
10    return arr;
11  }
```

Kode Sumber 4.2 Pembaca File

Array tersebut akan diparse sebanyak dua kali, pertama untuk mendapatkan titik koordinat yang akan diletakkan pada peta dan kedua untuk mendapatkan *IP Address* dan negara asal serangan yang akan ditampilkan pada tabel.

```
15  async function parse_file(arr)
16  {
17    const map = new Map();
18    for (let i=0; i<arr.length; i++) {
19      let lat_degree = read_coordinate(arr[i].Latitude);
20      let lon_degree = read_coordinate(arr[i].Longitude);
21      let ip_addr = arr[i].IP;
22      let attack_src = arr[i].Country;
23      let coordinates = lat_degree+","+lon_degree;
24
25      if (map.has(coordinates)) {
26        let size = map.get(coordinates).size + 1;
27        map.set(coordinates, {lat: lat_degree,
          lon: lon_degree, size: size});
28      } else {
29        map.set(coordinates, {lat: lat_degree,
          lon: lon_degree, size: 1});
30      }
31    }
32    return map;
33  }
```

Kode Sumber 4.3 Pengurai titik koordinat

```
53  async function parse_file_ip(arr)
54  {
55    const map = new Map();
56    for (let i=0; i<arr.length; i++)
57    {
58      let ip_addr = arr[i].IP;
59      let attack_src = arr[i].Country;
60
61      if (map.has(ip_addr)) {
62        let count = map.get(ip_addr).count + 1;
63        map.set(ip_addr, {ip: ip_addr, count: count});
64      } else {
65        map.set(ip_addr, {ip: ip_addr, count: 1});
66      }
67    }
68    return map;
69  }
```

Kode Sumber 4.4 Pengurai IP Address

Titik koordinat yang digunakan di dataset menggunakan koordinat GPS (Geographic Coordinate System) . Untuk dapat ditampilkan di peta Threat Map maka harus dikonversi terlebih dahulu dari bentuk String menjadi Floating Point.

```
function read_coordinate(data)
{
  stage = STAGE.DEGREE;
  let deg = 0.0;
  let min = 0.0;
  let sec = 0.0;
  let south = false;
  for (let i = 0; i<data.length; i++) {
    if (data[i] === 'd') { stage = STAGE.MINUTE; continue; }
    if (data[i] === '\'') { stage = STAGE.SECOND; continue; }
    if (data[i] === '\"') { stage = STAGE.CARDINAL; continue; }
    switch (stage) {
      case STAGE.DEGREE:
        deg = deg*10 + (+data[i]); break;
      case STAGE.MINUTE:
        min = min*10 + (+data[i]); break;
      case STAGE.SECOND:
        sec = sec*10 + (+data[i]); break;
      case STAGE.CARDINAL:
        if (data[i] === 's' || data[i] === 'S') { south = true;}
        break;
      default:
        break;
    }
  }
  let sum = degree_decimal(deg, min, sec);
  if (south === true) { sum *= -1; }
  return sum;
}
```

Kode Sumber 4.5 Konversi String Koordinat menjadi Floating point

Dari String koordinat akan terdapat tiga nilai koordinat, yaitu: derajat, menit dan detik. Dari ketiga nilai akan didapatkan nilai *Degree Decimal* dengan

perhitungan seperti berikut.

```
function degree_decimal(degree, minute, second)
{
      return degree + (minute/60) + (second/3600);
}
```

Kode Sumber 4.6 Penghitung nilai Koordinat

4.3.2 Data Visualizer

Dari data yang sudah dibaca, maka Threat Map dapat menampilkan titik-titik serangan pada peta dengan ukuran masing-masing titik bergantung pada jumlah serangannya.

```
async function render_points(hash, map)
{
  hash.forEach( (v,k) => {
    L.circle(
      [v.lat, v.lon],
      {radius:500*v.size, color: '#7db37d'}
    ).addTo(map);
    L.circle(
      [v.lat, v.lon],
      {radius:500, color: '#7db37d'}
    ).addTo(map);
  });
}
```

Kode Sumber 4.7 Penampil titik serangan

Dan untuk data IP Address dan asal serangan ditampilkan pada tabel yang dibuat dengan sebagai berikut:

```
async function leaderboard_func(hash_ip)
{
   let table = document.createElement('table');
   let thead = document.createElement('thead');
   let tbody = document.createElement('tbody');

   table.appendChild(thead);
   table.appendChild(tbody);
```

```
83    document.getElementById('leaderboard').appendChild(table);
84    let row_1 = document.createElement('tr');
85    let heading_1 = document.createElement('th');
86    heading_1.innerHTML = 'Index';
87    let heading_2 = document.createElement('th');
88    heading_2.innerHTML = 'Target IP Address';
89    let heading_3 = document.createElement('th');
90    heading_3.innerHTML = 'Attack Frequency';
91
92    row_1.appendChild(heading_1);
93    row_1.appendChild(heading_2);
94    row_1.appendChild(heading_3);
95    thead.appendChild(row_1);
96
97    let index = 1;
98    hash_ip.forEach( (v,k) => {
99      let row_2 = document.createElement('tr');
100     let row_2_data_1 = document.createElement('td');
103     row_2_data_1.innerHTML = index;
104     let row_2_data_2 = document.createElement('td');
105     row_2_data_2.innerHTML = v.ip;
106     let row_2_data_3 = document.createElement('td');
107     row_2_data_3.innerHTML = v.count;
108
109     row_2.appendChild(row_2_data_1);
110     row_2.appendChild(row_2_data_2);
111     row_2.appendChild(row_2_data_3);
112     tbody.appendChild(row_2);
113
114     index += 1;
115     });
116 }
```

Kode Sumber 4.8 Pembuat tabel data

4.4 Testing

Pada bagian testing penulis akan menunjukan fitur-fitur yang sudah berhasil diimplementasikan pada aplikasi Threat Map dimana dalam melaksanakan testing ini digunakan 2 (dua) dataset. Dataset yang pertama menunjukkan titik yang banyak dalam wilayah Indonesia dimana setiap titik merepresentasikan lokasi acak, sedangkan dataset yang kedua menunjukkan beberapa titik yang memiliki frekuensi serangan yang besar agar dapat menampilkan kemampuan

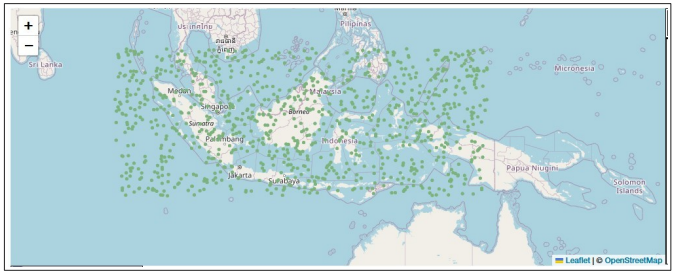
aplikasi untuk menunjukkan titik pada peta dengan ukuran bervariasi berdasarkan frekuensi serangan

Untuk mencapai tujuan testing aplikasi Threat Map ini, penulis menggunakan dataset yang penulis buat khusus dengan menggunakan script Lua. Dataset ini terdiri dari koordinat latitude dan longitude serta IP address unit yang diserang dan asal negara penyerang unit.

Gambar 4.3 Interface aplikasi Threat Map

4.4.1 Menampilkan titik serangan berjumlah besar di peta

Pada testing ini, menggunakan dataset berisi 1.000 titik serangan acak sekitar Indonesia yang didapatkan menggunakan pembangkit koordinat acak untuk tujuan testing aplikasi, maka aplikasi harus bisa menunjukan setiap titik pada peta.



Gambar 4.4 Tampilan aplikasi dengan data 1.000 titik serangan

4.4.2 Menampilkan titik serangan dengan frekuensi serangan yang besar

Pada testing ini, menggunakan dataset berisi data 1.105 serangan pada 3 titik di sekitar Indonesia yang didapatkan menggunakan pembangkit koordinat acak untuk tujuan testing aplikasi, maka aplikasi harus bisa menunjukan titik dengan ukuran berbanding dengan frekuensi serangan.

Gambar 4.5 Tampilan aplikasi dengan 4 titik serangan yang berat

4.4.3 Menampilkan daftar IP serangan berjumlah besar

Pada testing ini, menggunakan dataset pertama aplikasi menunjukan data serangan pada sebuah tabel. Tabel menunjukan IP Address unit yang diserang serta frekuensi serangannya. Jika jumlah IP Address sangat besar maka tabel dapat digerakkan menggunakan scroll wheel untuk melihat data yang lainnya

Index	Target IP Address	Attack Frequency
1	199.62.98.130	1
2	10.99.95.194	1
3	63.16.67.185	1
4	216.13.36.229	1
5	97.20.143.185	1
6	136.151.52.206	1
7	235.232.30.118	1
8	17.162.255.120	1
9	93.40.248.94	1
...	...	...
996	141.223.113.136	1
997	52.225.125.202	1
998	245.55.97.154	1
999	191.231.149.173	1
1000	19.178.126.184	1

Tabel 4.1 Data serangan 1.000 titik

4.4.4 Menampilkan daftar IP serangan dengan frekuensi serangan yang besar

Pada testing ini dengan menggunakan dataset kedua aplikasi menunjukan data serangan pada sebuah tabel. Tabel menunjukan IP Address unit yang diserang serta frekuensi serangannya.

Index	Target IP Address	Attack Frequency
1	164.24.2.1	337
2	126.78.16.4	335
3	172.5.1.51	328
4	192.0.0.4	105

Tabel 4.2 Data serangan 4 titik yang frekuen

4.5 Tampilan Aplikasi

Tampilan aplikasi Threat Map terdiri dari 3 komponen, yaitu: peta interaktif yang akan menunjukkan titik-titik serangan, tabel yang menampilkan data-data serangan dan interface yang menghubungkan dataset serangan dengan kedua komponen sebelumnya.

4.5.1 Dataset

Dataset yang digunakan merupakan dataset yang dibuat menggunakan *random number generation* yang berisi dengan koordinat global unit yang diserang yang teridiri koordinat latitude dan koordinat longitude, serta

alamat IP unit yang diserang dan sumber negara serangan.

	A	B	C	D	E
1	Index	Latitude	Longitude	IP	Country
2	1	6d17'51"S	106d49'56"E	64.0.0.1	PH
3	2	7d15'21"S	112d44'57"E	128.0.0.1	ID
4	3	6d17'51"S	106d49'56"E	64.0.0.1	ID
5	4	0d31'2"N	116d0'12"E	96.0.0.1	MY
6	5	6d17'51"S	106d49'56"E	64.0.0.1	PH
7	6	7d15'21"S	112d44'57"E	128.0.0.1	ID
8	7	6d55'54"S	107d46'41"E	160.0.0.1	ID
9	8	7d15'21"S	112d44'57"E	128.0.0.1	ID
10	9	6d55'54"S	107d46'41"E	160.0.0.1	ID
11	10	7d15'21"S	112d44'57"E	128.0.0.1	PH
12	11	6d55'54"S	107d46'41"E	160.0.0.1	ID
13	12	7d15'21"S	112d44'57"E	128.0.0.1	ID
14	13	7d15'21"S	112d44'57"E	128.0.0.1	CN
15	14	6d17'51"S	106d49'56"E	64.0.0.1	CN
16	15	7d15'21"S	112d44'57"E	128.0.0.1	MY
17	16	7d15'21"S	112d44'57"E	128.0.0.1	ID
18	17	0d31'2"N	116d0'12"E	96.0.0.1	ID
19	18	6d17'51"S	106d49'56"E	64.0.0.1	MY
20	19	6d17'51"S	106d49'56"E	64.0.0.1	CN

Gambar 4.6 sampel data dari dataset buatan

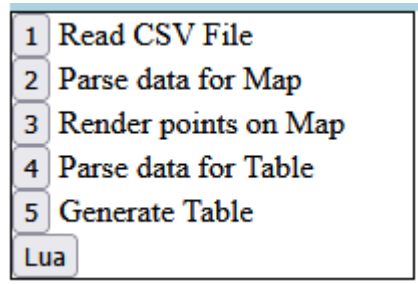
Dataset tersebut memiliki 5 unit yang diserang yang masing-masing terletak di Jakarta, Balikpapan, Surabaya, Bandung dan Makassar. Selain itu juga ada kode negara asal penyerang yang dipilih secara acak antara Indonesia, Malaysia, Filipina dan Cina namun data ini tidak digunakan dalam aplikasi.

No	Latitude	Longitude	Alamat IP	Lokasi Unit
1	6°17'51"S	106°49'56"E	64.0.0.4	Jakarta
2	0°31'2"N	116°0'12"E	96.0.0.4	Balikpapan
3	7°15'21"S	112°44'57"E	128.0.0.4	Surabaya
4	6°55'54"S	107°46'41"E	160.0.0.4	Bandung
5	5°13'52"S	119°35'25"E	192.0.0.4	Makassar

Tabel 4.3 Koordinat dan Alamat IP setiap Unit

4.5.2 Panel Start-up

Sebelum aplikasi dapat menampilkan data, pengguna harus memuat dan mengurai dataset dengan memencet tombol di panel start-up sesuai urutan tombol. Tombol terkahir yang berlabel “Lua” merupakan bekas pengembangan yang tidak ada fungsinya.



Gambar 4.7 Panel Start-up aplikasi

4.5.3 Peta Interaktif

Menggunakan library LeafletJS untuk javascript, aplikasi dapat menampilkan peta interaktif.

Pengguna dapat menggerakkan daerah yang ditampilkan dengan mengklik cursor pada peta dan menyeret berlawan arah terhadap daerah yang ingin dilihat. Lalu, pengguna juga dapat memperbesar atau memperkecil skala peta dengan menggunakan mouse wheel atau dengan tombol yang terletak di kiri atas peta.

Gambar 4.8 Tampilan peta menggunakan dataset buatan

4.5.4 Tabel Data

Dalam aplikasi terdapat tabel yang menunjukkan frekuensi serangan serta alamat IP unit yang diserang dari dataset yang digunakan.

Tabel data menggunakan baris label duplikat untuk kasus dimana dataset mengandung jumlah unit yang melebihi tinggi elemen tabel sehingga ketika pengguna scroll ke bawah maka label data masih terlihat.

Index	Target IP Address	Attack Frequencey

Index	Target IP Address	Attack Frequency
1	64.0.0.1	202
2	128.0.0.1	398
3	96.0.0.1	99
4	160.0.0.1	199
5	192.0.0.1	102

Gambar 4.9 Tampilan tabel data serangan

4.5.5 Pembahasan

Dari tampilan sebelumnya, dapat dilihat bahwa unit Surabaya mendapatkan serangan terbesar dengan 398 serangan diikuti dengan unit Jakarta dan Bandung dengan 199-202 serangan serta unit Balikpapan dan Makassar dengan serangan terkecil pada 99-102 serangan. Maka didapatkan rata-rata total 200 serangan dengan median 199 serangan.

Karena dataset hanya menyimpan informasi mengenai unit yang diserang tanpa menyimpan informasi penyerang, maka akan diasumsikan bahwa serangan dilakukan oleh berbagai sumber atau *hacker*

yang berbeda.

Berdasarkan data dan asumsi tersebut, maka ditemukan bahwa di antara 5 unit yang dimonitor, unit yang terletak di Surabaya adalah unit yang paling rentan. Dengan jumlah 398 serangan yang melebihi rata-rata sebanyak 198 serangan dan melebihi median sebanyak 199 serangan atau dua kali jumlah serangan median. Namun, penemuan ini bukan berarti bahwa unit yang lainnya tentu tidak rentan hanya bahwa unit yang menjadi sasaran terbesar bagi *hacker* adalah unit yang terletak di Surabaya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang didapat setelah melakukan pengembangan aplikasi Threat Map pada kegiatan Kerja Praktik di PT PLN Nusantara Power adalah sebagai berikut:

a. Pada penggunaan tools yang tidak familiar penulis mendapatkan hasil yang kurang bagus karena threat map cukup rumit untuk bisa diintegrasi dengan sistem keamanan. Setelah menggunakan tools yang familiar penulis mendapatkan hasil yang cukup bagus dan threat map bisa mudah diintegrasi dengan web yang ada.
b. Perencanaan adalah faktor yang sangat penting dalam membuat threat map, pemahaman yang baik pada tools yang akan digunakan sangat berpengaruh dengan hasil yang ingin dicapai.
c. Waktu 3 (tiga) bulan untuk menjalankan kerja praktik bisa membuat threat map yang dapat menjalankan fungsi dasar tetapi untuk membuat threat map yang bisa memunculkan lebih banyak data lagi dibutuhkan waktu yang lebih lama

5.2 Saran

Setelah 3 (tiga) bulan menjalankan kerja praktik penulis belum bisa mencapai hasil maksimal yang ingin dicapai, berikut adalah saran penulis untuk mengembangkan aplikasi :

a. Pelajari dan pahami dengan baik tools yang ingin digunakan dalam pengembangan perangkat lunak karena semakin familiar tools yang akan digunakan maka akan lebih cepat dan mudah mendapatkan hasil.

b. Rencanakan suatu proyek jauh sebelum mengimplementasikan sebuah solusi karena jika tidak melakukan perencanaan dengan baik maka akan menghadapi banyak halangan dan tundaan.

DAFTAR PUSTAKA

[1] Lange, K. (2023). Cyberattack Maps Explained: The Value & Limitations of Cyber Attack Maps. splunk.com. https://www.splunk.com/en_us/blog/learn/cyberattack-maps.html

[2] Minhaz, N. (2022). Cyber Threat Mapping. storymaps.arcgis.com. https://storymaps.arcgis.com/stories/8b3674949e38493ab3ae1c2ceab2d8fb

[3] PT. PLN Nusantara Power. (2024). TENTANG KAMI - PLN Nusantara Power. plnnusantarapower.co.id. https://www.plnnusantarapower.co.id/tentang-kami/(accessed April, 2025)

[4] Proxsis IT. (2025). Tren Ancaman Siber di Indonesia Meningkat? Berikut Fakta yang Harus Diketahui. it.proxsisgroup.com. https://it.proxsisgroup.com/tren-ancaman-siber-di-indonesia-meningkat-berikut-fakta-yang-harus-diketahui/

[5] Corbo, A. (2022). What Is HTML? builtin.com. https://builtin.com/software-engineering-perspectives/html

[6] Jordana, A. (2025).What Is JavaScript: A Beginner's Guide to the Basics of JS. hostinger.com. https://www.hostinger.com/tutorials/what-is-javascript

[7] Jadhav, S. (2023). JavaScript for Data Visualization: A Guide to D3.js. medium.com. https://medium.com/@siddhantjadhav445/javascript-for-data-visualization-a-guide-to-d3-js-f7e45c3ddd67

[8] Swadia, S. (2021). A Beginner's Guide to Creating a Map Using Leaflet.js. sitepoint.com. https://www.sitepoint.com/leaflet-create-map-beginner-guide/

[Halaman ini sengaja dikosongkan]

BIODATA PENULIS

Nama : Schaquille Devlin Aristano Tempat, Tanggal Lahir : Jakarta, 15 Oktober 2003 Jenis Kelamin : Laki-laki
Agama : Islam
Status : Belum Menikah
Telepon 081250575200
Email : schaquildevlin@gmail.com

PENDIDIKAN FORMAL
2021 – sekarang : S1 Teknik Informatika ITS 2018 – 2021 : SMA Al-Azhar 19 Ciracas
2015 – 2018 : SMP Nasional KPS
2009 – 2015 : SD Nasional KPS

AKADEMIS
Kuliah : Departemen Teknik Informatika – FTEIC , ITS
Angkatan : 2021
Semester : 8 (Delapan)
IPK : 3.04