

Dokumen Laporan Gangguan

Incident report

WEB DEFAACEMENT
TRANSJAKARTA-CSIRT

[Area Kantor Pusat Offline]
[18 Juli 2022]

Divisi Digital & IT
PT. Transportasi Jakarta

HASIL PENANGANAN INSIDEN

"NAMA INSIDEN"

I. Dokumentasi Insiden Keamanan Siber

| | | |
|-------------------------|---|--|
| Waktu Pelaporan Insiden | : | |
| Identitas Pelapor | : | |
| Hal Pelaporan | : | |
| Aset yang dilaporkan | : | |
| Screenshot | : | |

II. Mitigasi

Mitigasi merupakan kegiatan yang dilakukan guna mengurangi dampak secara meluas pada sebuah insiden yang terjadi

Menjelaskan Teknik mitigasi yang sudah dilakukan apa saja :

1. Xxx

2. Xxx

III. Hasil Identifikasi

Bukti-bukti yang ada pada insiden ini berupa:

Melampirkan gambar atau file yang ditemukan

IV. Analisis Hasil Identifikasi

Menjelaskan analisis hasil identifikasi, diantaranya

1. Aktivitas yang tercatat dalam bukti insiden

2. Menjelaskan insiden yang telah terjadi dan perkiraan tanggal kejadian insiden
3. Alamat IP yang melakukan anomaly terhadap website
4. Jenis software dan tools yang digunakan pelaku
5. Analisis kemungkinan pelaku masuk melalui port/serangan apa

V. Rekomendasi Penanganan Insiden

Menjelaskan tindakan yang dilakukan untuk mitigasi