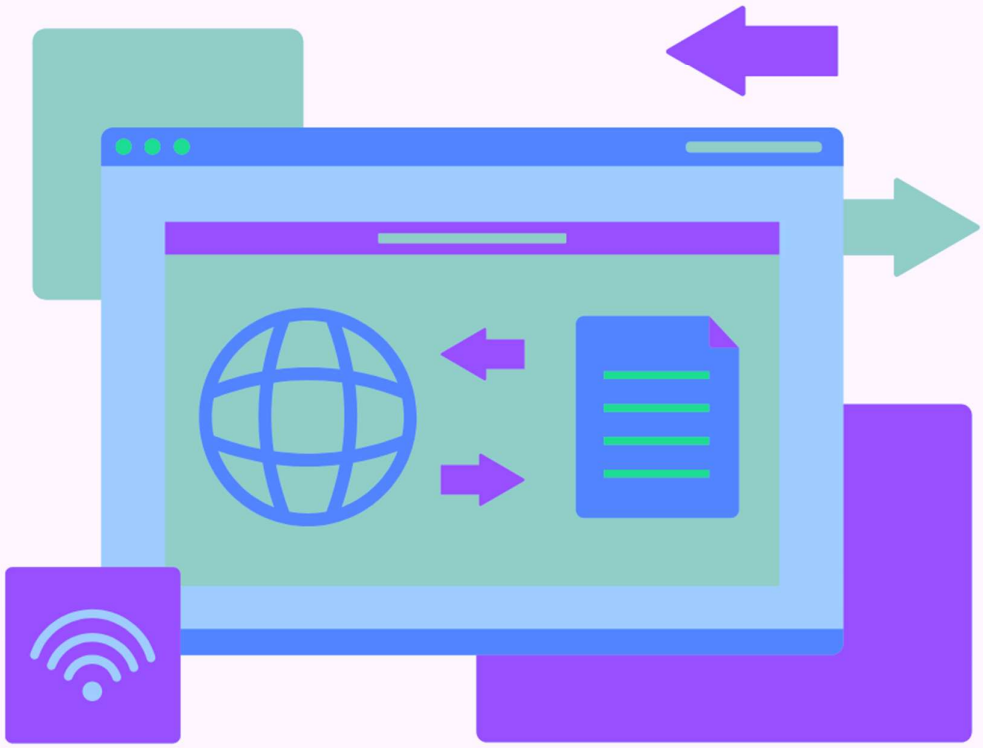
diskominfo KOTA SUKABUMI - spirit of sharing -

OPEN DATA KOTA SUKABUMI

PANDUAN

PANDUAN PENANGANAN INSIDEN SERANGAN WEB DEFACEMENT



Bidang Statistik, Persandian dan Keamanan Informasi

Diskominfo Kota Sukabumi

diskominfo_sukabumikota | Pemerintah kota Sukabumi | @pemkot_sukabumi | sukabumikota.go.id

KATA PENGANTAR

Puji syukur kehadirat Allah SWT, atas segala limpahan rahmat, nikmat serta karunia-Nya yang tak ternilai dan tak dapat dihitung sehingga kami dapat menyelesaikan penyusunan "Panduan Penanganan Insiden Serangan *Web Defacement*". Panduan ini disusun dalam rangka memberikan acuan bagi pihak yang berkepentingan dalam penanganan insiden serangan *Web Defacement*. Panduan ini berisikan langkah-langkah yang harus diambil apabila terjadi serangan *Web Defacement*, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan serangan. Panduan ini tentu saja masih banyak kekurangan dan masih jauh dari kesempurnaan karena keterbatasan ilmu dan referensi kami. Untuk itu, kami selalu berusaha melakukan evaluasi dan perbaikan secara berkala agar bisa mencapai hasil yang lebih baik lagi.

Akhir kata, kami ucapkan terima kasih kepada segala pihak yang telah membantu dalam penyusunan penduan ini.

Sukabumi,

Kepala Dinas Komunikasi dan Informatika

Ditandatangani Secara Elektronik Oleh:

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KOTA SUKABUMI,

Ir. Hj. ENDAH ARUNI, M.T.
Pembina Tk. I / IVb
NIP. 196707091997032005

1. Tahapan Penanganan

Tahap	Deskripsi
1. Deteksi	Mendeteksi perubahan tampilan situs web yang mencurigakan atau tidak sah.
2. Validasi	Memastikan insiden adalah defacement, bukan perubahan yang sah.
3. Isolasi	Mengisolasi sistem terdampak dari jaringan publik untuk mencegah penyebaran.
4. Analisis	Mengidentifikasi metode serangan, titik masuk, dan konten yang diubah.
5. Eradikasi	Menghapus akses penyerang dan menambal celah keamanan yang dimanfaatkan.
6. Pemulihan	Mengembalikan situs ke versi normal dan aman dari backup terpercaya.
7. Pelaporan	Menyusun laporan insiden untuk audit internal dan otoritas terkait.
8. Pencegahan	Memperkuat keamanan aplikasi dan server serta edukasi tim pengelola.

2. Penjelasan Detail Tiap Tahap

1. Deteksi

- Pantau tampilan web secara rutin atau gunakan monitoring otomatis.
- Laporan dari pengguna juga bisa menjadi indikator awal.

2. Validasi

- Bandingkan dengan versi yang sah dari situs.
- Cek timestamp, log, dan riwayat perubahan file.

3. Isolasi

- Putuskan koneksi ke internet.
- Blokir akses eksternal ke sistem yang terdampak.

4. Analisis

- Audit log web server.
- Identifikasi celah (misal: file upload, XSS, RFI, LFI).
- Lacak IP atau metode akses.

5. Eradikasi

- Hapus file/skrip tidak sah.
- Perbaiki permission dan celah yang ditemukan.
- Reset kredensial akun.

6. Pemulihan

- Restore dari backup yang valid.
- Verifikasi tidak ada backdoor tertinggal.
- Tes fungsi web secara menyeluruh.

7. Pelaporan

- Catat waktu kejadian, dampak, bukti digital, dan respons yang dilakukan.
- Laporkan ke manajemen dan jika perlu ke CSIRT/BSSN.

8. Pencegahan

- Gunakan WAF dan patch sistem.
- Audit kode secara berkala.
- Terapkan prinsip least privilege.
- Latih tim pengelola keamanan.

3. Flowchart Visual