Pengelolaan Computer Security Incident Response Team (CSIRT)

Magelang, 10 September 2024

Setyo Budi Prabowo, S.ST

setyo.budi@bssn.go.id

0819 3229 9540

SMA N 1 Muntilan

Sekolah Tinggi Sandi Negara

Pengalaman Unit Kerja

- Direktorat Pembinaan Persandian, Lemsaneg (2011-2013)
- Direktorat Pengamanan Sinyal, Lemsaneg (2014-2016)
- Biro Hukum PHKH, Sekretaris Utama, BSSN (2017 – 2018)
- Direktorat Proteksi Ekonomi Digital, BSSN (2019 - 2021)
- Direktorat Operasi Keamanan dan Pengendalian Informasi, BSSN (2022 s.d sekarang)

Pengalaman Tugas Operasi

- Operasi Pengamanan Gelombang Frekuensi
- Operasi Pengamanan VVIP
- Operasi Counter Surveillance (Dalam dan Luar Negeri)
- Operasi Keamanan Sistem Informasi
- Operasi Keamanan Laut

Dasar Hukum

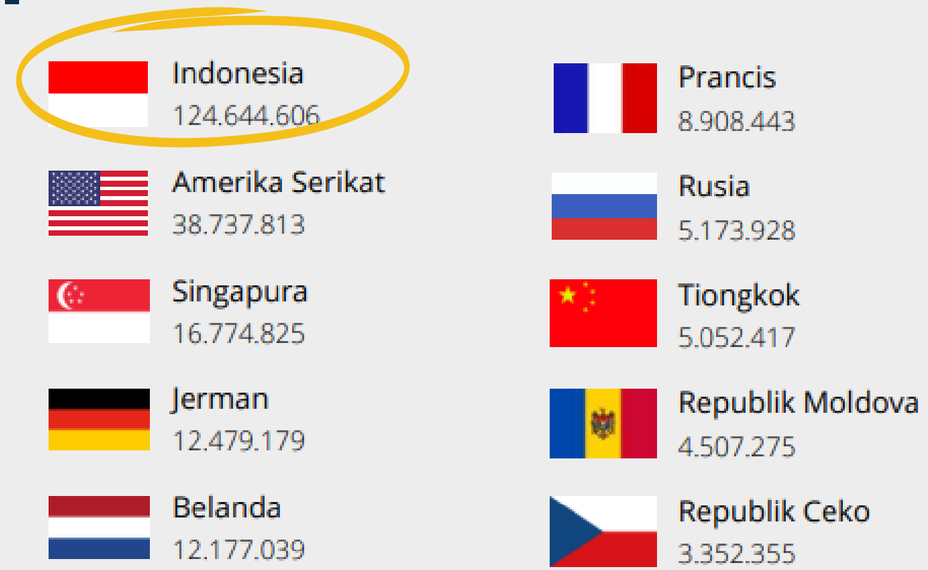
1. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah
2. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber
3. Peraturan Badan Siber Dan Sandi Negara Nomor 1 Tahun 2024 Tentang Pengelolaan Insiden Siber

2023

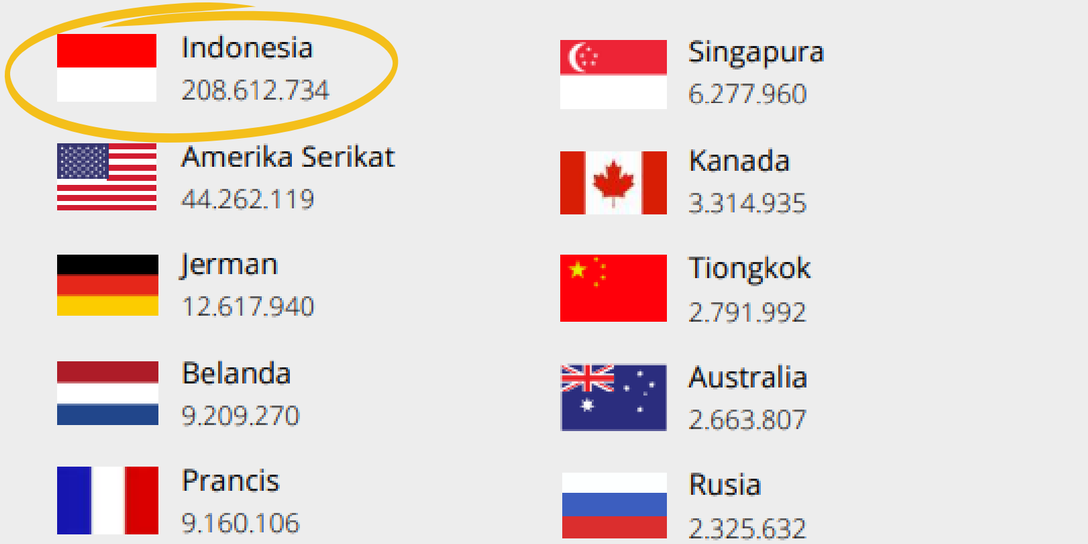
Trafik Anomali

Serangan Siber di Dunia

TOP 10 SUMBER ANOMALI



TOP 10 TUJUAN ANOMALI

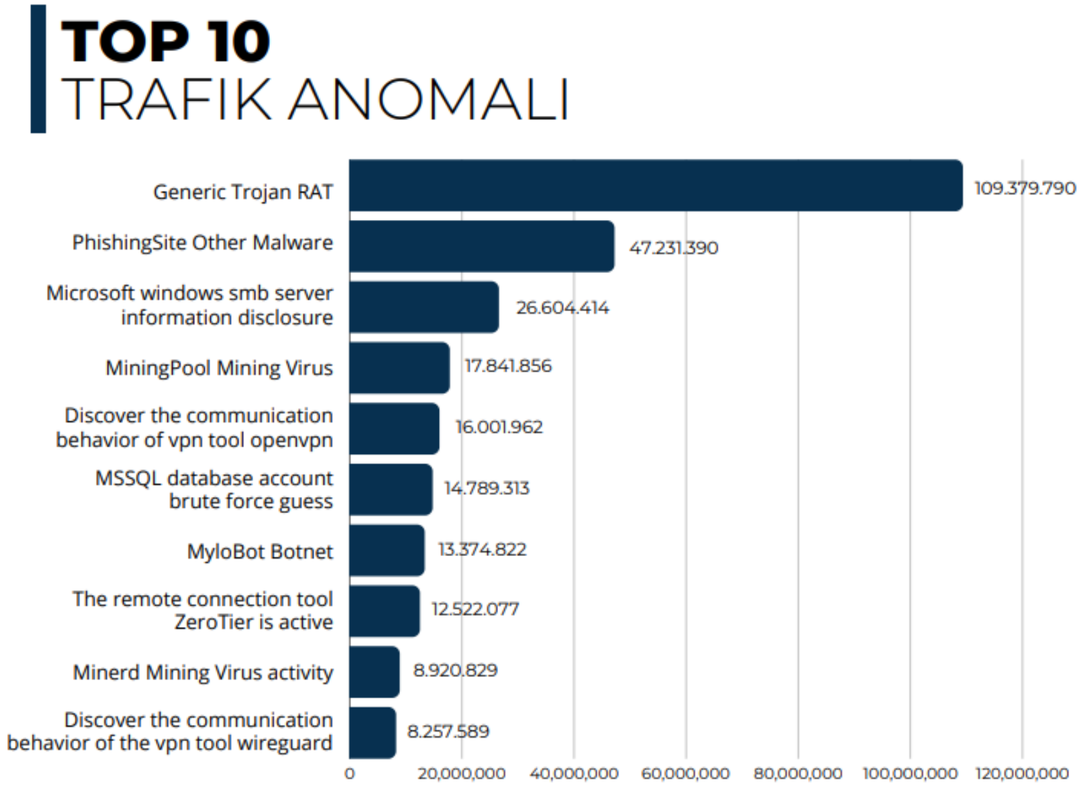


Sumber: Lanskap Keamanan Siber Indonesia 2023 Id-SIRTII/CC-BSSN

2023

Trafik Anomali

Serangan Siber di Indonesia



Total trafik anomali di Indonesia selama tahun 2023 adalah **403.990.813 anomali**. dengan jenis trafik anomali tertinggi yaitu **Generic Trojan RAT.**

Aktivitas anomali trafik ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi.

Sumber: Lanskap Keamanan Siber Indonesia 2023 Id-SIRTII/CC-BSSN

2023

Rekapitulasi dan Notifikasi

Dugaan Insiden Siber

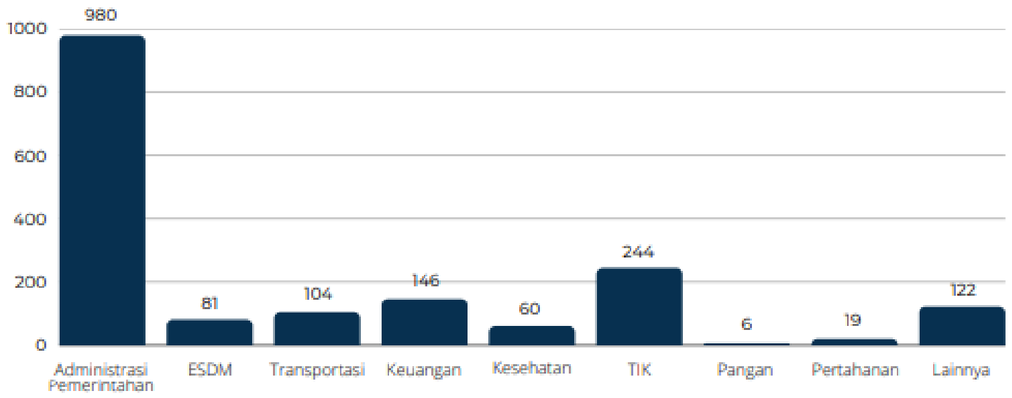
1.762
NOTIFIKASI TERKIRIM

Tim Pusat Kontak Siber BSSN mengirimkan sebanyak **1.762 notifikasi** indikasi insiden siber ke berbagai sektor.

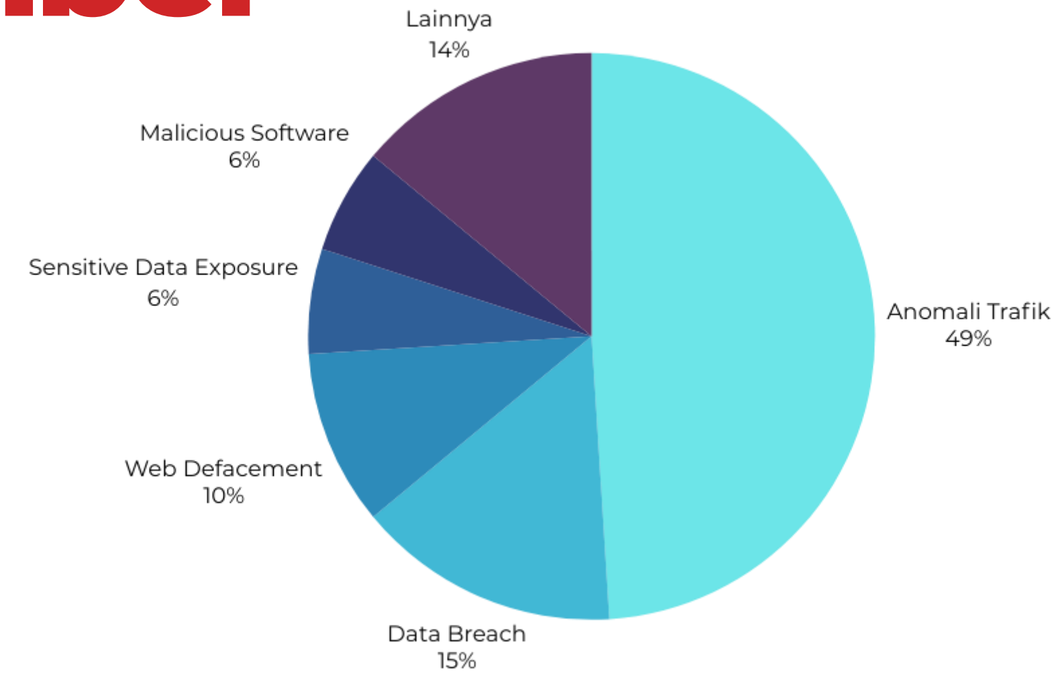
43% | **755 Notifikasi** Direspon

57% | **1007 Notifikasi** Tidak direspon

REKAPITULASI NOTIFIKASI BERDASARKAN SEKTOR



Tim Pusat Kontak Siber BSSN mengirimkan sebanyak 1.762 notifikasi indikasi insiden siber ke berbagai sektor.
980 notifikasi dikirimkan ke Sektor Administrasi Pemerintahan



Dari 1.762 Notifikasi terkirim, didapatkan hasil Top 5 Klasifikasi Indikasi Insiden yang dinotifikasi oleh BSSN yaitu:

- Anomali Trafik : 858,
- Data Breach : 268,
- Web Defacement : 172,
- Senisitive Data Exposure : 113,
- Malicious Software : 104.

Sumber: Lanskap Keamanan Siber Indonesia
2023 Id-SIRTII/CC-BSSN

2023

Pemantauan
Cyber Threat Intelligence

347

Dugaan Insiden Siber

Sebaran Jenis Insiden

Penelusuran Dugaan Insiden
199 laporan

Pemantauan Proaktif Dugaan Insiden
228 laporan

Sektor Terdampak	Jumlah
Adm. Pemerintahan	186
Lainnya	60
Keuangan	38
Transportasi	24
ESDM	18
TIK	5
Kesehatan	5
Pangan	5
Pertahanan	2

Hasil pemantauan Cyber Threat Intelligence (CTI) ditemukan sebanyak **347 dugaan insiden siber** di antaranya yaitu kebocoran data, ransomware, web defacement, indikasi potensi serangan DDoS, dan pemantauan proaktif dugaan insiden siber
186 data diantaranya menyerang Administrasi Pemerintahan

Sumber: Lanskap Keamanan Siber Indonesia 2023 Id-SIRTII/CC-BSSN

2023

Pemantauan
Cyber Threat Intelligence

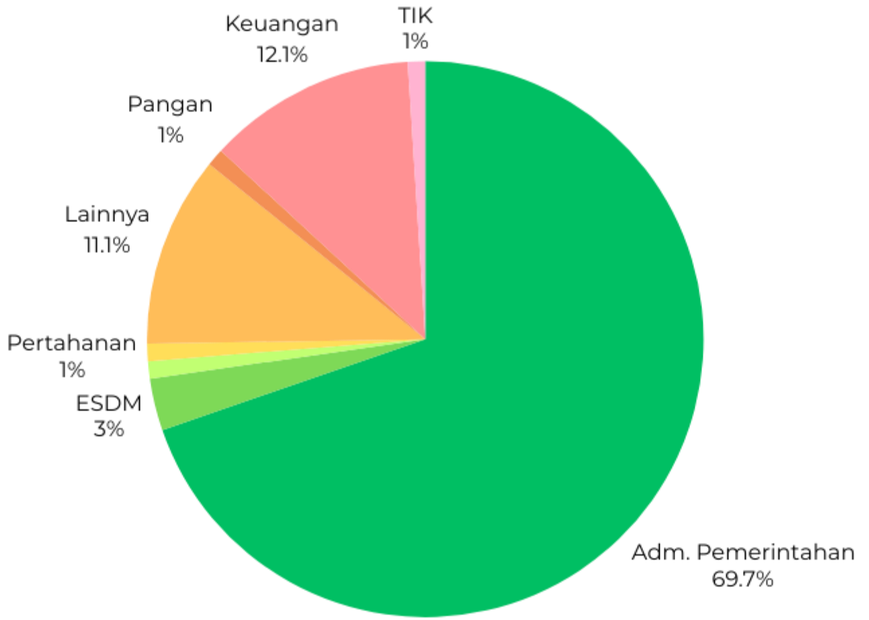
WEB DEFACEMENT

Serangan web defacement merupakan serangan yang dilakukan untuk mengeksploitasi situs web atau server web yang rentan dengan memanfaatkan kerentanan dari sistem sehingga threat actor dapat merusak, memodifikasi, atau menghapus konten halaman web yang telah diretas.

167	Adm. Pemerintahan	7	Kesehatan
12	Lainnya	3	Pertahanan

Selama tahun 2023, sektor yang paling banyak terkena serangan web defacement adalah sektor **Administrasi Pemerintahan** dengan jumlah kasus sebanyak 167 kasus.

KEBOCORAN DATA



Sektor Administrasi Pemerintahan tercatat memiliki jumlah insiden **terbanyak** dengan total **71 kasus**. Data ini menunjukkan bahwa sektor **Administrasi Pemerintahan merupakan area yang paling banyak terdampak**, yang memerlukan perhatian khusus dalam manajemen risiko dan peningkatan keamanan siber.

Sumber: Lanskap Keamanan Siber Indonesia 2023 Id-SIRTII/CC-BSSN

2023

Lesson Learned

TOP 3 INSIDEN SIBER

Web Defacement

1. Melakukan Security Hardening Pada OS Server
2. Meningkatkan Keamanan dan Manajemen Autentikasi Pengguna yang Mengakses Server Secara Remote
3. Pemantauan Aktivitas Situs
4. Pengelolaan Akses
5. Kesadaran Pengguna
6. Menangani Kelemahan yang Ada dan Mengaktifkan Kembali Layanan Web
7. Melakukan Penguatan Keamanan pada CMS yang Sedang Digunakan

Ransomware

1. Pembaruan Sistem dan Perangkat Lunak
2. Pelatihan Security Awareness Kepada Pengguna
3. Penggunaan Perangkat Keamanan dan Deteksi Ancaman Siber
4. Pengelolaan Hak Akses dengan Bijak
5. Backup dan Pemulihan Data yang Teratur
6. Menguatkan Keamanan Supply Chain
7. Mengamankan Remote Desktop Protocol (RDP)

Sumber: Lanskap Keamanan Siber Indonesia 2023 Id-SIRTII/CC-BSSN

2023

Lesson Learned

TOP 3 INSIDEN SIBER

Data Breach

1. Menetapkan Kebijakan Penggunaan password yang Kuat
2. Melakukan Edukasi Terhadap Pengguna Sistem
3. Melakukan Audit Akun Sistem dan Aplikasi
4. Menonaktifkan Port Layanan yang Tidak Digunakan
5. Memvalidasi Data Terkait Insiden yang Terjadi
6. Melakukan Penguatan Keamanan atau Pembaruan Pada Sistem yang Terdampak

“Organizations have a responsibility to protect the data they collect from their customers and employees.”

European Union General Data Protection Regulation (GDPR)

Sumber: Lanskap Keamanan Siber Indonesia 2023 Id-SIRTII/CC-BSSN

Tata Kelola

Keamanan Informasi

1. Keamanan sumber daya teknologi informasi;
2. Keamanan akses kontrol;
3. Keamanan data dan informasi;
4. Keamanan sumber daya manusia;
5. Keamanan jaringan;
6. Keamanan surat elektronik;
7. Keamanan pusat data; dan/atau
8. Keamanan komunikasi.

Pengamanan

Sistem Elektronik

Identifikasi

Kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.

Deteksi

Melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.

Proteksi

Kegiatan mitigasi risiko dan penerapan pelindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.

Penanggulangan dan pemulihan

Penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Computer Security Incident Response Team (CSIRT)

1. CSIRT Nasional
2. CSIRT Sektoral
3. CSIRT Organisasi
4. CSIRT Khusus

FUNGSI

1. Pemberian peringatan terkait Keamanan Siber;
2. Perumusan panduan teknis penanganan Insiden Siber;
3. Pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;
4. Pemilahan (triage) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani;
5. Penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan; dan
6. Penyelenggaraan fungsi lainnya sesuai kebutuhan.

Jenis CSIRT	CSIRT Nasional	CSIRT Sektoral	CSIRT Organisasi	CSIRT Khusus
Yang Membentuk	BSSN	K/L yang berwenang melakukan pengawasan pada sektornya (PP Nomor 71 Tahun 2019 tentang PSTE); BSSN -> Gov CSIRT	setiap organisasi Penyelenggara Sistem Elektronik	organisasi pemerintah ataupun nonpemerintah
Gangguan yang dilayani	tingkat nasional: Min. 2 sektor & @2 organisasi; > 1/2 jumlah organisasi dalam 1 (satu) sektor	Insiden Siber pada sektornya: • Min. 2 (dua) organisasi max. ½ jumlah organisasi di sektor	Insiden Siber pada lingkup organisasi atau institusi	Insiden Siber untuk kebutuhan yang bersifat khusus: • kewilayahan; • komunitas tertentu; • pelanggan berbasis layanan komersial; • pelanggan produk tertentu; dan/atau • kegiatan dalam jangka waktu tertentu.

museum sandi

Layanan CSIRT

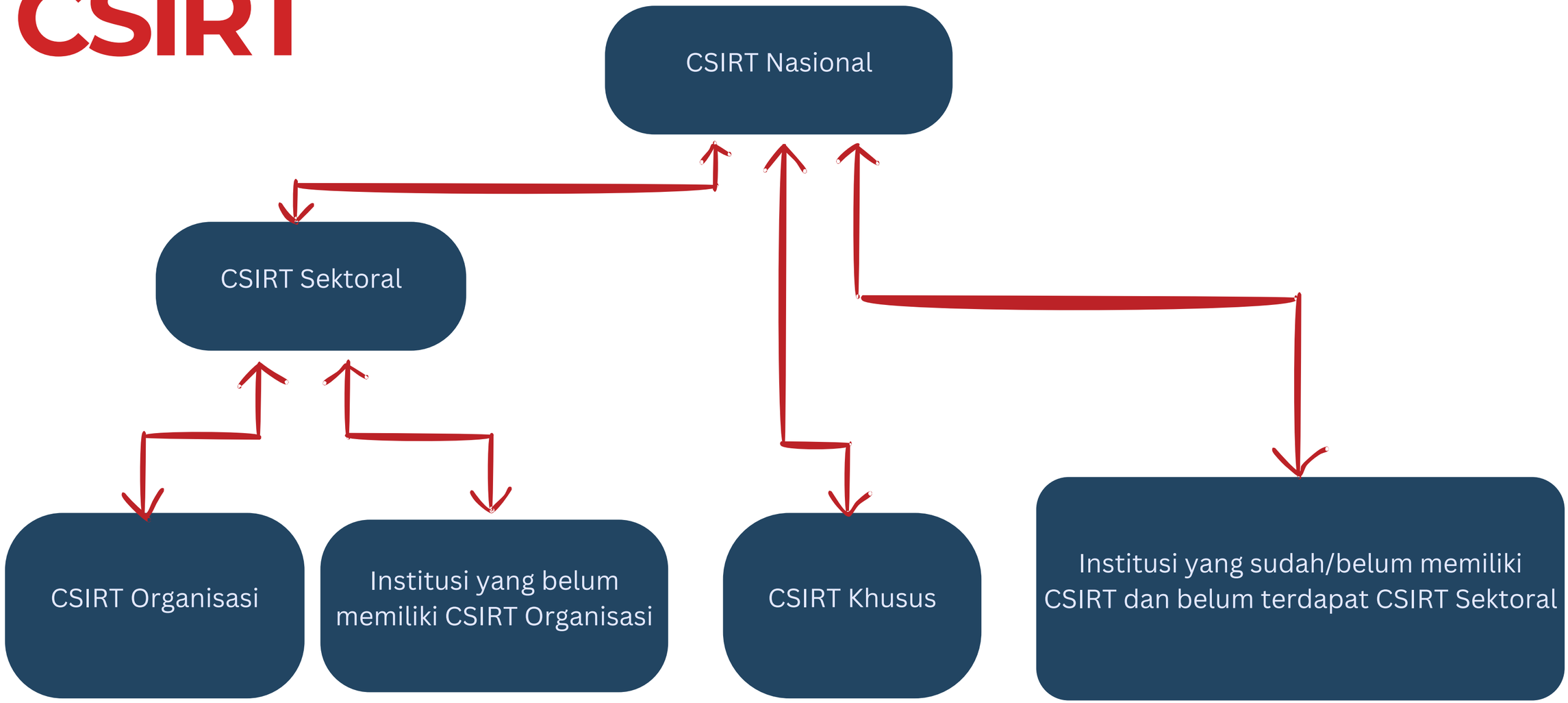
LAYANAN UTAMA

- Pemberian peringatan terkait keamanan siber; dan
- Pengelolaan Insiden Siber (menerima, menanggapi, dan menganalisis Insiden Siber)

LAYANAN TAMBAHAN

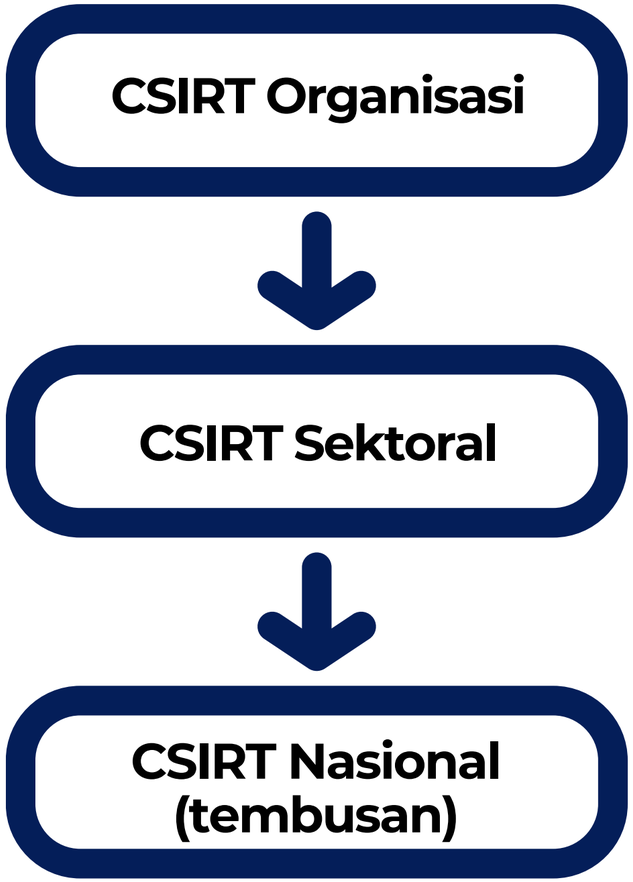
- Penanganan kerentanan sistem elektronik;
- Penanganan artefak digital;
- Pemberitahuan hasil pengamatan potensi ancaman;
- Pendeteksian serangan;
- Analisis risiko keamanan siber;
- Konsultasi terkait kesiapan penanganan Insiden Siber; dan/atau
- Pembangunan kesadaran dan kepedulian terhadap keamanan siber.

Alur Koordinasi
CSIRT



Pelaporan

Insiden Siber



paling lambat 1 x 24 (satu kali dua puluh empat) jam setelah ditemukan adanya Insiden Siber

Insiden Siber ditentukan berdasarkan:

- Hasil deteksi Tim CSIRT;
- Analisis Insiden Siber berdasarkan aduan dari pemilik sistem atau masyarakat; dan/atau
- Pemberian peringatan dari CSIRT Nasional setelah terkonfirmasi sebagai Insiden Siber.

Laporan Insiden Siber, paling sedikit memuat:
a. informasi kontak pelapor;
b. deskripsi Insiden Siber;
c. kronologi Insiden Siber; dan
d. dampak serangan.

museum sandi

1 Terjadi Insiden Siber

Insiden Siber dapat berupa:

- Web Defacement
- SQL Injection
- Malware
- Ransomware
- DDos
- Ilegal Access

2 Melapor kepada CSIRT Organisasi (Internal)

Melaporkan insiden siber yang terjadi kepada CSIRT Organisasi melalui kontak resmi, misalnya melalui:

- Telepon
- Email
- Chat Mesenger
- dsb

3 Penanganan Insiden oleh CSIRT Organisasi

- Verifikasi laporan berupa insiden atau hanya kesalahan konfigurasi
- Jika insiden siber, CSIRT Organisasi melakukan penanganan sesuai SOP yang berlaku

4 CSIRT Organisasi meminta bantuan CSIRT Sektoral

- Jika insiden tidak dapat tertangani, CSIRT Organisasi dapat meminta bantauan CSIRT Sektoral dengan cara:
- Pengumpulan Bukti insiden (foto/screenshot /log)
- Menghubungi kontak resmi CSIRT Sektoral

5 Penanganan Insiden bersama CSIRT Sektoral

- CSIRT Sektoral bersama CSIRT Organisasi berkolaborasi dalam penanganan insiden siber.
- Kontak resmi CSIRT Sektoral BSSN
- Telp: 021-78833610
- Email: bantuan70@bssn.go.id

museum sandi

Penanggulangan dan Pemulihan **Insiden Siber**

01 Menyusun perencanaan penanggulangan dan pemulihan Insiden Siber;

02 Menganalisis dan melaporkan Insiden Siber

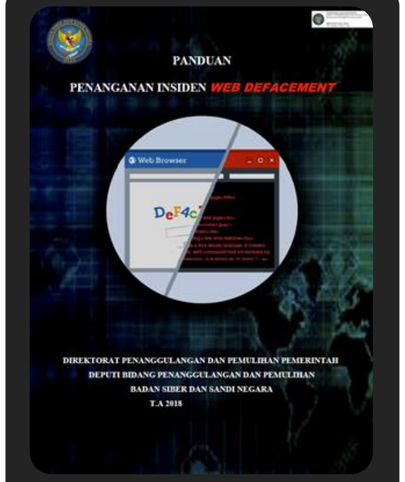
03 Melaksanakan penanggulangan dan pemulihan Insiden Siber;

04 Meningkatkan keamanan setelah terjadinya Insiden Siber.

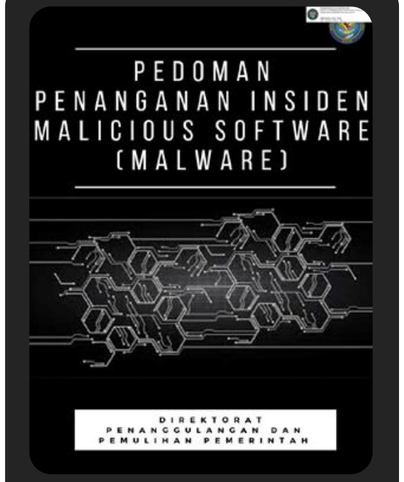
Panduan Teknis Penanganan **Insiden Siber**

https://drive.bssn.go.id/s/j86W2Q2dywGL4oo

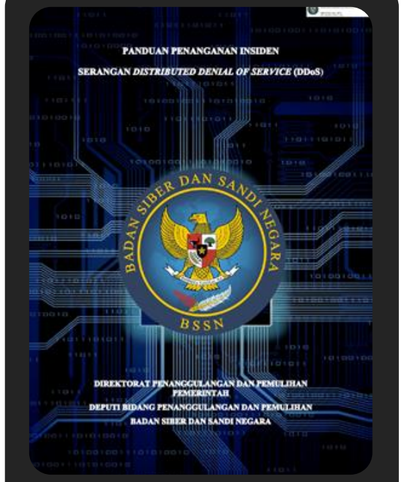
Pedoman Teknis Penanganan Ransomware



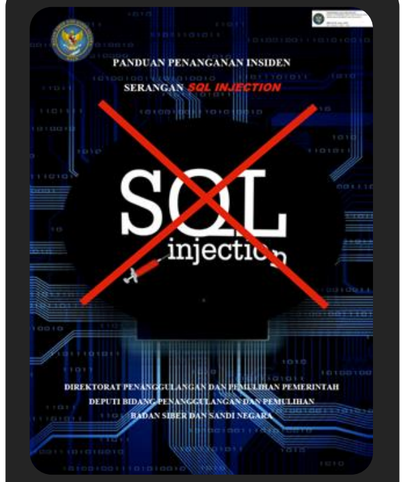
Pedoman Teknis Penanganan Web Defacement



Pedoman Teknis Penanganan Malware



Pedoman Teknis Penanganan DDoS



Pedoman Teknis Penanganan SQL Injection

Pedoman Teknis Penanganan SQL Injection

museum sandi

“Kunci utama penanganan Insiden adalah KOORDINASI dan KOLABORASI antar berbagai pihak berkepentingan”

museum sandi

Terima Kasih

"Ingatlah bahwa,
Kechilafan Satu Orang Sahadja
Tjukup Sudah Menjebabkan
Keruntuhan Negara"

(dr. Roebiono Kertopati)