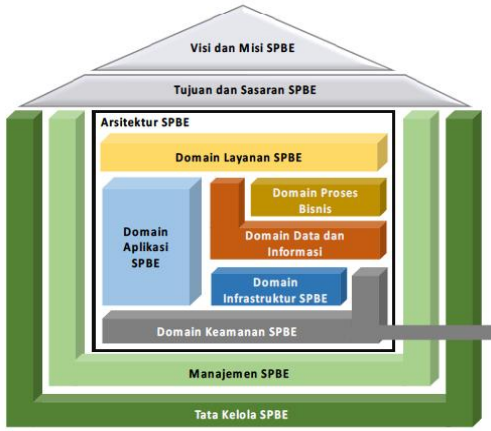
DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN MAGELANG

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

KOTA MUNGKID, 18 DESEMBER 2023

AMANAT REGULASI TERKAIT PEMBENTUKAN CSIRT



Referensi Arsitektur Keamanan SPBE

- Standar Keamanan
- Penerapan Keamanan
- Kelaikan Keamanan

- Edukasi Kesadaran Keamanan SPBE
- Identifikasi Kerentanan Keamanan SPBE
- Peningkatan Keamanan SPBE
- Penanganan Insiden Keamanan SPBE
- Audit Keamanan SPBE

Computer Security Incident Response Team (CSIRT)

Sumber : Perpres 95/2018 SPBE dan Perpres 132/2022 Arsitektur SPBE Nasional

Diatur

PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 10 TAHUN 2020
TENTANG
TIM TANGGAP INSIDEN SIBER

SALINAN

PRESIDEN
REPUBLIK INDONESIA

Diamanatkan

PERATURAN PRESIDEN REPUBLIK INDONESIA
NOMOR 82 TAHUN 2022
TENTANG
PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL

Pasal 12

(1) Badan membentuk Tim Tanggap Insiden Siber nasional sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a.

(2) Kementerian atau Lembaga membentuk Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b.

(3) Penyelenggara IIV membentuk Tim Tanggap Insiden Siber organisasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c.

GAMBARAN CSIRT DI INDONESIA

Apa itu CSIRT ?

CSIRT
Computer Security Incident Response Team

Organisasi / tim yang bertanggung jawab untuk menerima, meninjau, dan menanggapi laporan dan aktivitas insiden keamanan siber

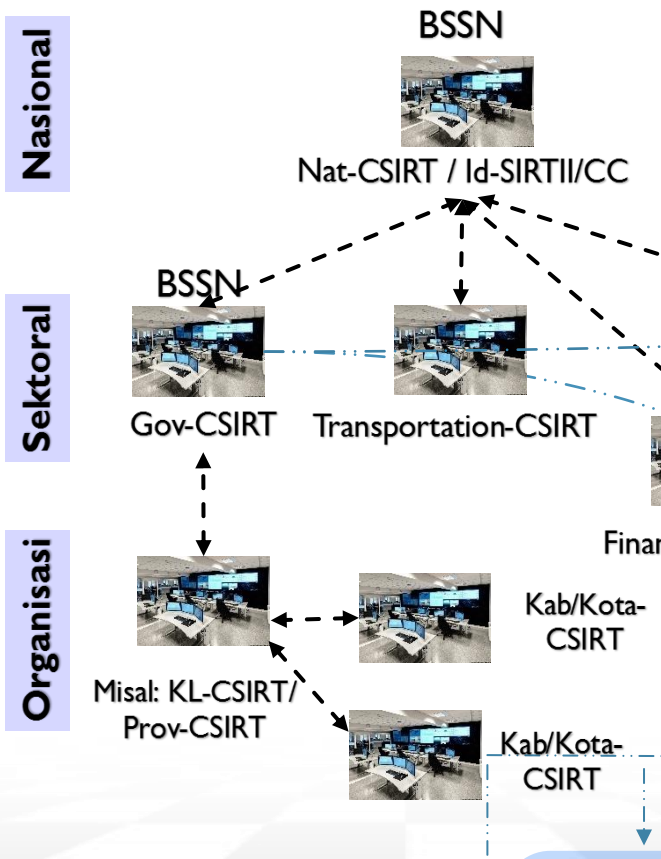
Fungsi CSIRT

Memberikan layanan CSIRT sesuai dengan kebutuhan penanganan insiden siber di ruang lingkup tanggungjawabnya.
Layanan CSIRT berupa :

1. Layanan Utama
   a. Pemberian peringatan terkait keamanan siber
   b. Penanganan insiden siber
2. Layanan Tambahan
   Penambahan Layanan disesuaikan dengan kebutuhan organisasi

Kenapa diperlukan CSIRT

Data BSSN menunjukkan pada tahun 2022 terdapat 976.429.996 Anomali trafik di Indonesia. Hal ini dipicu salah satunya oleh peningkatan implementasi layanan berbasis elektronik, shg memicu peningkatan aktivitas di ruang siber.



BSSN

- *Deputi Bidang Operasi Keamanan Siber dan Sandi / NSOC BSSN berperan sebagai Nat-CISRT / Id-SIRTII/CC yang akan berkolaborasi dengan CSIRT Internasional.*

Tahun 2019, BSSN telah melaunching Gov-CSIRT melalui Kepka BSSN Nomor 570 Tahun 2018 Tanggal 20 Des 2018 tentang CSIRT

Perpres No 18 Tahun 2020 ttg RPJMN 2020 - 2024

PRESIDEN REPUBLIK INDONESIA

Rencana Kerja Pemerintah: Penguatan NSOC dan Pembentukan 121 CSIRT KL/D (87 KL dan 34 Pemprov)

Dimana CSIRT berada dalam suatu organisasi ?

CSIRT merupakan bagian dari penyelenggaraan keamanan TI. Oleh karenanya CSIRT dapat berada pada unit kerja atau Dinas yang memiliki kewenangan penyelenggaraan layanan dan keamanan TI di suatu organisasi.

TAHAPAN PEMBENTUKAN CSIRT

1 Asistensi CSIRT

- *Memahami regulasi dan Kebijakan CSIRT*
- *Memahami tujuan CSIRT*
- *Memahami model dan mekanisme kerja CSIRT*
- *Memahami SDM CSIRT*
- *Memahami Layanan-Layanan CSIRT*
- *Memahami Pendanaan CSIRT*

EDUKASI

PERENCANAAN

PENERAPAN

OPERASIONAL & KOLABORASI

2 Perencanaan CSIRT

- *Perumusan Visi & Misi CSIRT*
- *Perumusan Struktur Organisasi CSIRT*
- *Identifikasi Layanan CSIRT*
- *Identifikasi Kebutuhan SDM CSIRT*
- *Identifikasi Kebutuhan Perangkat / Tools CSIRT*
- *Penyusunan Kebijakan, Pedoman, Panduan*
- *Penyusunan Rencana Kerja & Anggaran*

3 Penerapan CSIRT

- *Pengangkatan Tim CSIRT*
- *Pemenuhan Perangkat/Tools CSIRT*
- *Penerapan Kebijakan, Pedoman, Panduan, SOP*
- *Deklarasi CSIRT*
- *Registrasi CSIRT*
- *Launching CSIRT*

Launching CSIRT

4 Operasional & Kolaborasi CSIRT

CSIRT mempunyai pengalaman penanganan insiden dan berkolaborasi dengan CSIRT lain

Pengangkatan Tim CSIRT dapat melalui SK / Surat Perintah

- *Website CSIRT*
- *Perangkat Komunikasi (Email, Telp, Fax, dsb)*
- *Sistem Ticketing Aduan Insiden Siber*
- *Sistem Monitoring (IDS/SIEM)*
- *Tools Respon Insiden*

- *Panduan Pelaporan Insiden Siber*
- *Panduan Penanganan Insiden Web Defacement*
- *Pedoman Penanganan Insiden Malware*
- *dsb*

Deklarasi CSIRT umumnya mengguanakan RFC 2350

Mengirim berkas registrasi CSIRT ke BSSN melalui email / paket pos.

Bagi instansi yang telah melakukan registrasi CISRT, BSSN akan memberikan peningkatan kapabiitas SDM CSIRT, dalam bentuk :

- *Cyber Drill*
- *Workshop Pengelolaan CSIRT*
- *Pelatihan-pelatihan*

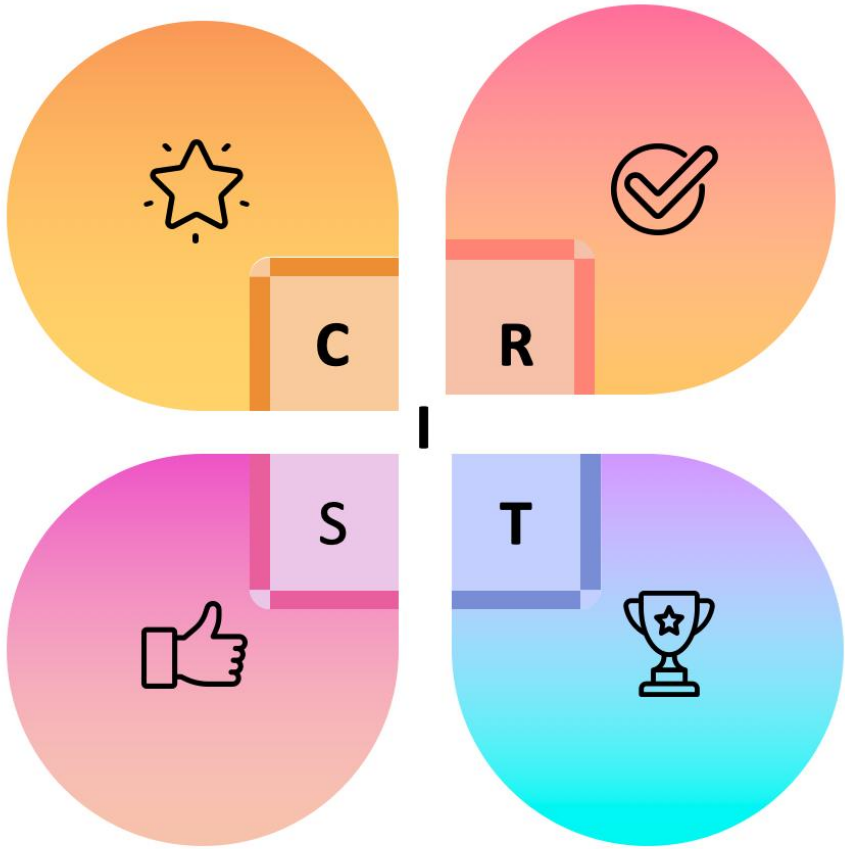
PENYELENGGARAAN CSIRT

Tata Kelola CSIRT

Pemenuhan dan Implementasi Kebijakan, Pedoman dan Prosedur CSIRT

Peningkatan CSIRT

- Peningkatan Kompetensi CSIRT melalui :
  - Pelatihan
  - Workshop
  - Cyber Drill
- Pemenuhan Perangkat CSIRT



Layanan CSIRT

- Pemberian Peringatan terkait Keamanan Siber
- Penanganan insiden siber
- Layanan Tambahan CSIRT

Publikasi CSIRT

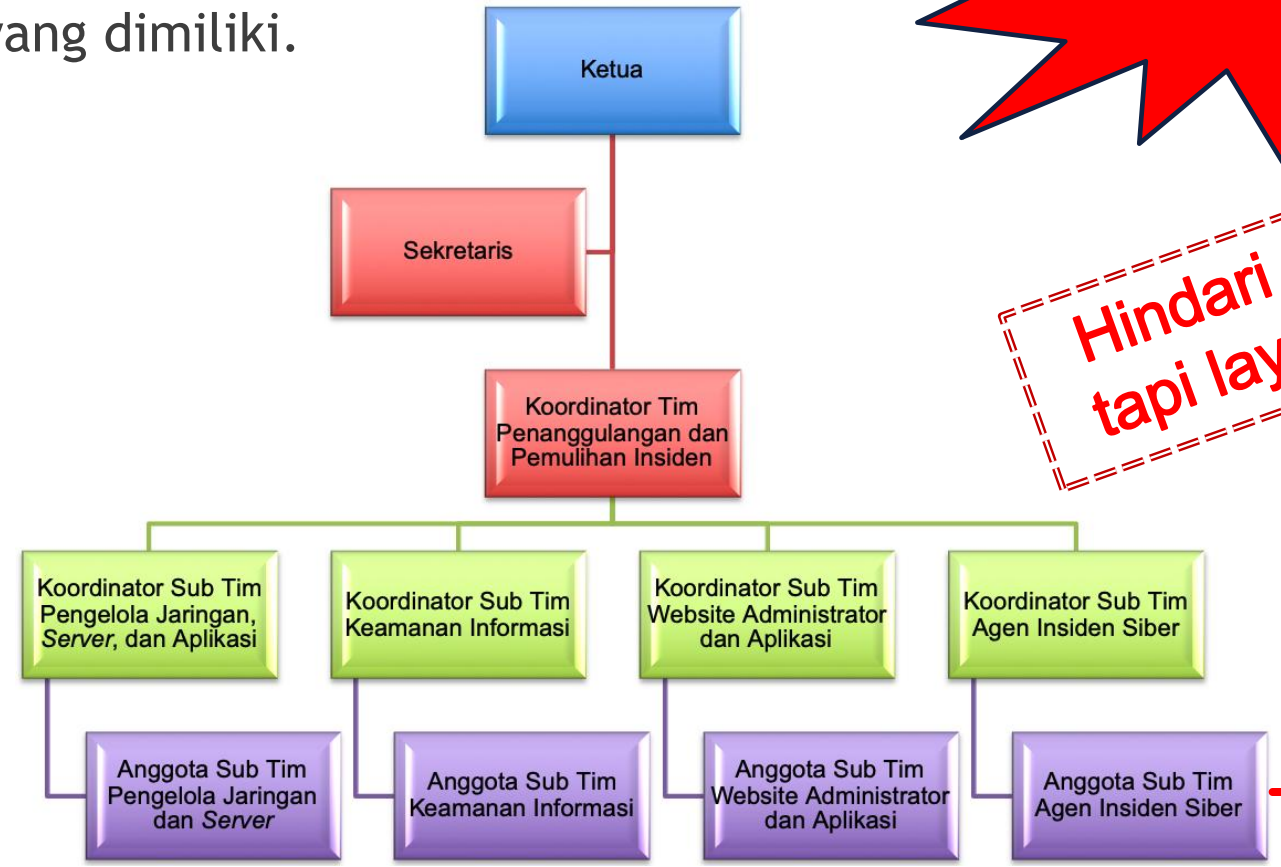
- Sosialisasi
- Diseminasi
- Literasi

STRUKTUR CSIRT

Tim CSIRT dibentuk berdasarkan layanan yang diberikan kepada konstituen dan keahlian staf yang dimiliki.

CONTOH

Hindari struktur dibuat tapi layanan tidak ada.



Agen Siber melibatkan pemilik sistem elektronik

PERSIAPAN INSTANSI PEMERINTAH YANG DIBENTUK CSIRT

Penyiapan Dokumen

Dokumen Pendaftaran CSIRT :

- SK tentang Tim CSIRT;
- Formulir Registrasi Tim Tanggap Insiden Siber;
- RFC 2350;
- Sumber Daya Penyelenggara CSIRT;
- Pernyataan Narahubung CSIRT.

Dokumen Aduan Siber

- Form Aduan Siber
- Formulir Penanganan Insiden Siber
- Format Laporan Penanganan Insiden Siber

Mendaftarkan CSIRT

Metode pendaftaran

Melalui email : registrasi.ttis@bssn.go.id

dan cc : kss.pemda@bssn.go.id

PERSIAPAN INSTANSI PEMERINTAH YANG MEMBENTUK CSIRT

- Penyiapan Teknis
  - Penyiapan Website CSIRT
  - Penyiapan perangkat dan tools respon insiden
- Implementasi
  - Implementasi Sistem Ticketing Aduan Siber
  - Implementasi Sistem Monitoring

PENYIAPAN DOKUMEN PENDUKUNG

Link Dokumen Pendukung :
https://s.id/KelengkapanCSIRT

Template SK	Draft SK Walikota/Bupati/Sekda
Dokumen Pendaftaran	Formulir Registrasi
	Template RFC 2350
	Sumber Daya Penyelenggara CSIRT
	Surat Pernyataan Narahubung
Dokumen Panduan Teknis	Instalasi SIEM (Wazuh)
	Instalasi Ticketing System (OSTicket)
	Panduan Pembangkitan Kunci Publik/Privat
Template Form Penanganan Insiden	Format Penanganan Insiden
	Formulir Laporan Penanganan Insiden
	Formulir Aduan Siber
Contoh Dok Pendaftaran dan Video	Contoh Dokumen Pendaftaran
	Contoh Video Launching CSIRT

MEDIA PUBLIKASI CSIRT

Media Publikasi CSIRT, **minimal** memuat informasi :

- ❑ Profil CSIRT
  - ❑ Nama CSIRT
  - ❑ Layanan CSIRT
- ❑ Informasi RFC2350
  - ❑ Dokumen RFC2350
  - ❑ Kunci Publik PGP
- ❑ Kontak
  - ❑ Alamat Email CSIRT
  - ❑ Alamat Hotline CSIRT

Minimal Kebutuhan Perangkat :

- ❑ RAM 2 GB
- ❑ Harddisk 100GB
- ❑ 2 Core CPU

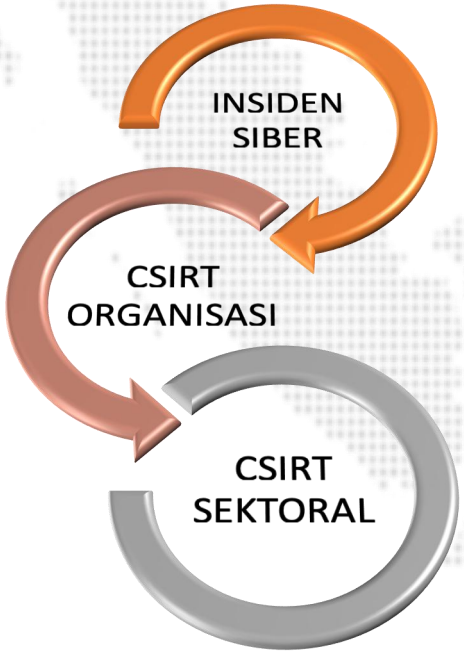
TINGKAT MATURITAS PENANGANAN INSIDEN SIBER

Instrumen Tingkat Maturitas Penanganan Insiden (TMPI) merupakan sebuah alat untuk memetakan tingkat kesiapan pemangku kepentingan dalam mengelola insiden siber secara cepat, tepat, efektif, dan mandiri oleh organisasi melalui identifikasi, pengukuran, dan mitigasi risiko serta meminimalisir dampak yang terjadi akibat insiden siber.

PERAN OPD DALAM TIM CSIRT KABUPATEN MAGELANG

- ✓ Pemantauan terhadap keamanan sistem elektronik di masing-masing Perangkat Daerah
- ✓ Inventarisasi aset Perangkat Daerah masing-masing, termasuk risikonya
- ✓ Penanganan insiden siber di lingkup Perangkat Daerah atau eskalasi penanganan insiden siber ke MagelangKab-CSIRT
- ✓ Pelaporan insiden siber ke MagelangKab-CSIRT menyertakan Log dan bukti kejadian
- ✓ Literasi/ edukasi terkait keamanan siber di internal Perangkat Daerah
- ✓ Berbagi Informasi terkait keamanan siber di lingkup Pemerintah Kota Magelang

PELAPORAN DAN PENANGANAN INSIDEN SIBER



1 Terjadi Insiden Siber

Insiden Siber dapat berupa kejadian berikut:

- *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 CSIRT Organisasi, misalnya melalui:

- *Telepon*
- *Email*
- *Chat Messenger*
- *dsb*

3 Penanganan Insiden oleh CSIRT Organisasi

- *POC memverifikasi apakah hal tsb insiden atau hanya kesalahan konfigurasi*
- *Jika merupakan insiden siber, maka tim CSIRT Organisasi akan melakukan penanganan insiden siber sesuai SOP yang berlaku*

4 CSIRT Organisasi meminta bantuan CSIRT Sektoral

Jika insiden tidak dapat tertangani, tim CSIRT Organisasi dapat meminta bantuan CSIRT Sektoral, dengan cara sbb:

- *Melakukan pengumpulan bukti insiden, misal: foto, screenshot, dan log insiden*
- *Menghubungi CSIRT Sektoral melalui kontrak resmi CSIRT Sektoral. Misal: BSSN*

5 Penanganan Insiden bersama CSIRT Sektoral

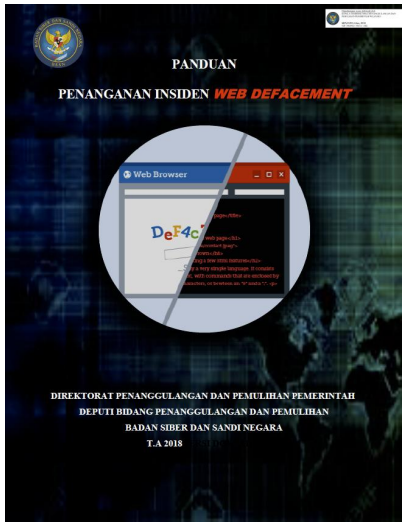
- *CSIRT Sektoral bersama CSIRT Organisasi berkolaborasi dalam penanganan insiden siber.*

- *Kontak resmi CSIRT Sektoral BSSN*
  Telp: 021 – 78833610
  Email: bantuan70@bssn.go.id

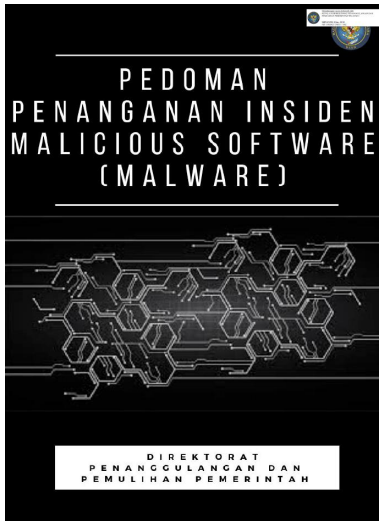
PANDUAN TEKNIS PENANGANAN INSIDEN SIBER

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

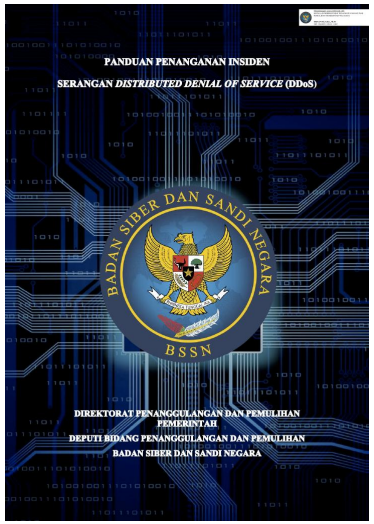
Pedoman Teknis Penanganan Ransomware



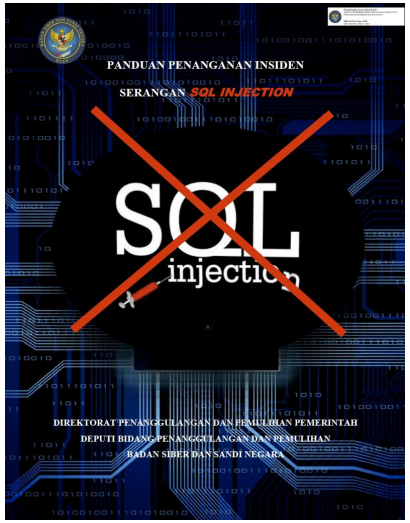
Pedoman Teknis Penanganan Web Defacement



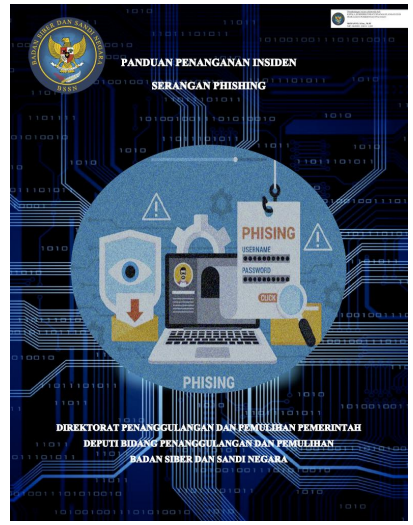
Pedoman Teknis Penanganan Malware



Pedoman Teknis Penanganan DDoS



Pedoman Teknis Penanganan SQL Injection



Pedoman Teknis Penanganan Phising

Cyber Security is a Shared Responsibility and it's Boils Down to this : in Cyber Security, the More Systems We Secure, the More Secure We All are.

Keamanan siber adalah tanggung jawab bersama dan intinya adalah : dalam keamanan siber, semakin banyak sistem yang kita amankan, semakin aman kita semua.

by Jeh Charles Johnson (US Secretary of Homeland Security from 2013 to 2017)

BADAN SIBER & SANDI NEGARA

TERIMA KASIH