BADAN SIBER DAN SANDI NEGARA

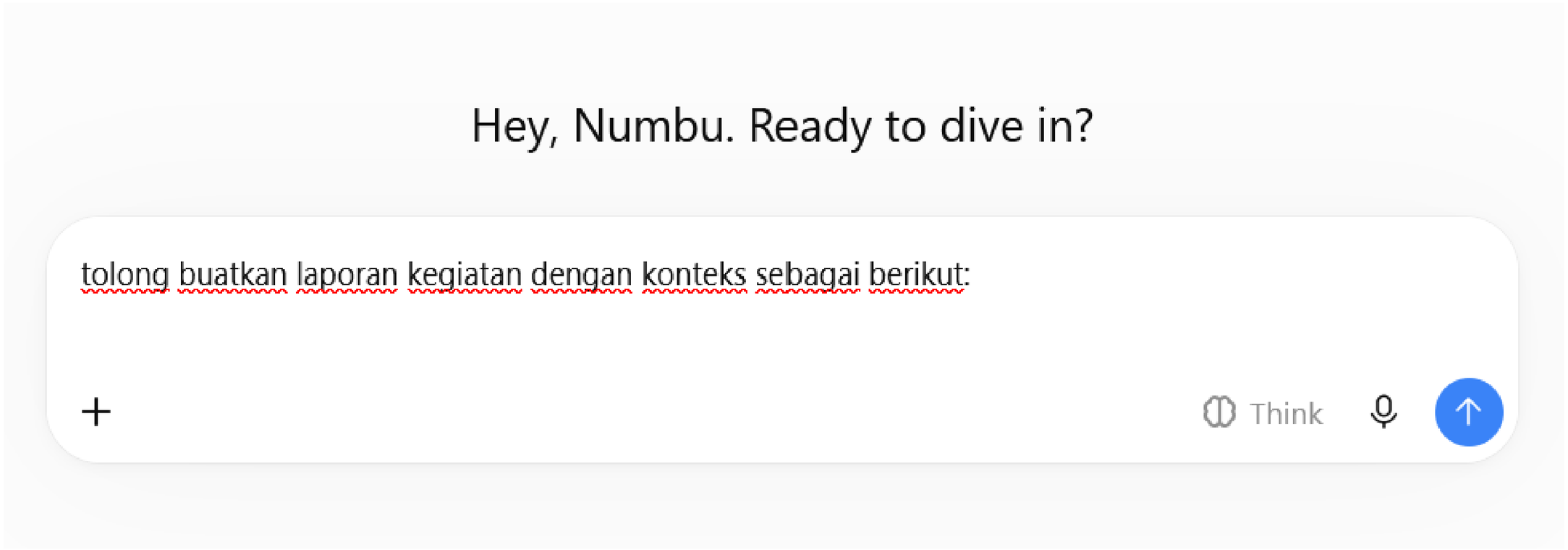
Tren Ancaman, Peran CSIRT, Mekanisme Pelaporan dan Koordinasi Insiden Siber

Literasi Data dan Keamanan Informasi

2 November 2026 | Kota Magelang

Reikal Taupaani, S.Tr.TP, M.T
Sandiman Muda - Direktorat KSS Pemerintah Daerah

Sudah Sejauh Apa kita Memanfaatkan AI?



Peralihan Peran AI menjadi Operator Serangan

Ancaman Tradisional

- Eksekusi manual dan berurutan.
- Membutuhkan keahlian teknis tinggi.
- Siklus eksploitasi memakan waktu berminggu-minggu.

Agentic AI (2026)

- Eksekusi kampanye serangan mandiri dan paralel.
- Reconnaissance otomatis pada infrastruktur publik.
- Eksploitasi multi-vektor selesai dalam hitungan jam.

Apa itu TTIS/CSIRT?



sekelompok orang yang bertanggung jawab mencegah dan menangani Insiden Siber pada lingkup organisasi atau institusi

Amanat Regulasi terkait TTIS/CSIRT

Pasal 41

(1) Setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan SPBE.

(2) Dalam menerapkan Keamanan SPBE dan menyelesaikan permasalahan Keamanan SPBE, pimpinan Instansi Pusat dan kepala daerah dapat melakukan konsultasi dan/atau koordinasi dengan kepala lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

(3) Penerapan Keamanan SPBE harus memenuhi standar teknis dan prosedur Keamanan SPBE.

(4) Ketentuan lebih lanjut mengenai standar teknis dan prosedur Keamanan SPBE diatur dengan Peraturan Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

- Perpres 95 Tahun 2018 ttg SPBE

Bagian Keempat

Pengelolaan Insiden Siber

Pasal 11

(1) Penanganan Insiden Siber dilaksanakan oleh Tim Tanggap Insiden Siber.

(2) Tim Tanggap Insiden Siber sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. Tim Tanggap Insiden Siber nasional;
   b. Tim Tanggap Insiden Siber sektoral; dan
   c. Tim Tanggap Insiden Siber organisasi.

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.

- Perpres 82 tahun 2022 ttg Perlindungan Infrastruktur Informasi Vital

Pasal 8

(1) Perencanaan sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf c dilakukan oleh pelaksana teknis Keamanan SPBE.

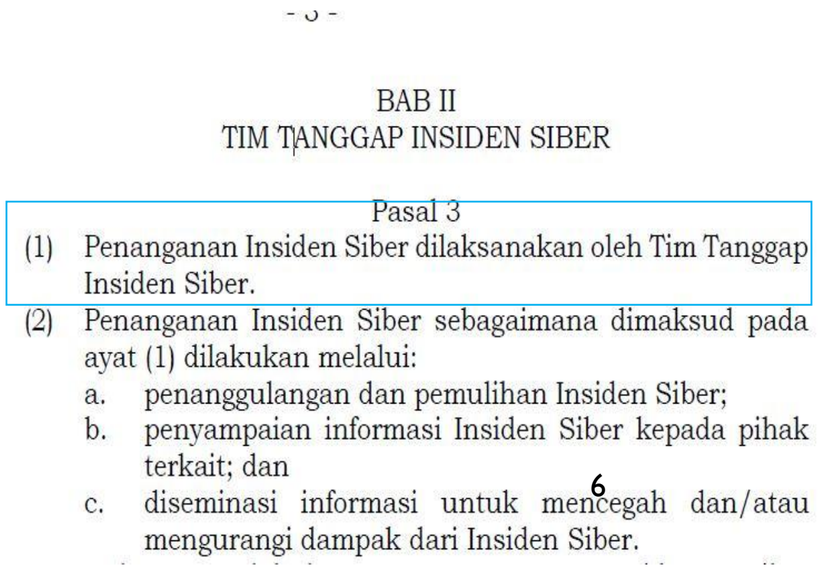
(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
   a. program kerja Keamanan SPBE yang disusun berdasarkan kategori risiko Keamanan SPBE; dan
   b. target realisasi program kerja Keamanan SPBE.

(3) Program kerja Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a paling sedikit meliputi:
   a. edukasi kesadaran Keamanan SPBE;
   b. penilaian kerentanan Keamanan SPBE;
   c. peningkatan Keamanan SPBE;
   d. penanganan insiden Keamanan SPBE; dan
   e. audit Keamanan SPBE.

(4) Kategori risiko Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a ditentukan sesuai dengan ketentuan peraturan perundang-undangan.

- Peraturan BSSN 4 tahun 2021 ttg Pedoman MKI SPBE

Amanat Regulasi terkait TTIS/CSIRT part 2



- 5 -

BAB II
TIM TANGGAP INSIDEN SIBER

Pasal 3

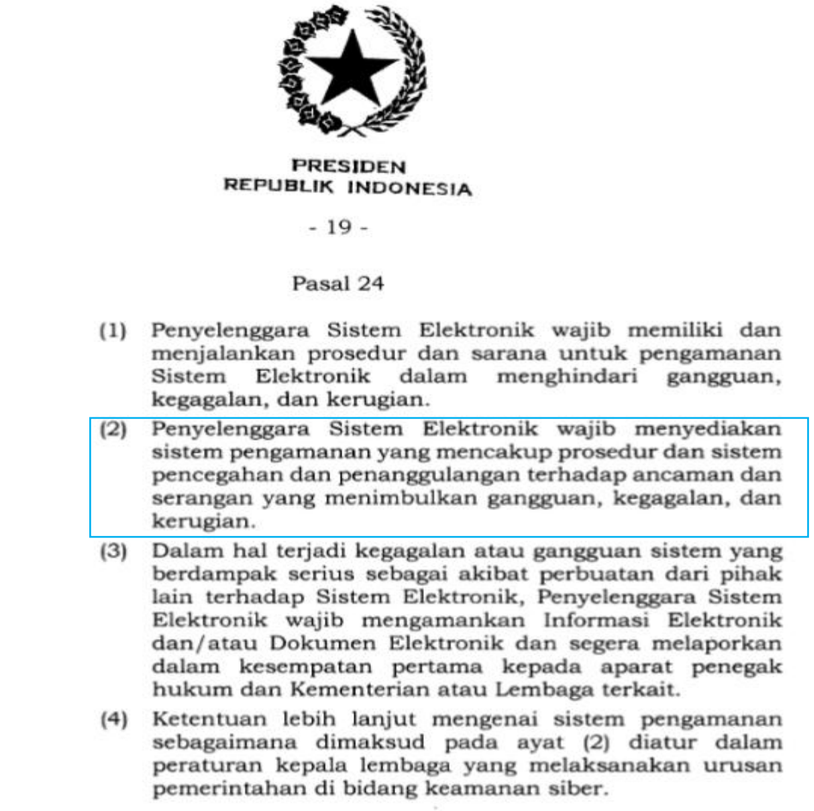
(1) Penanganan Insiden Siber dilaksanakan oleh Tim Tanggap Insiden Siber.

(2) Penanganan Insiden Siber sebagaimana dimaksud pada ayat (1) dilakukan melalui:
   a. penanggulangan dan pemulihan Insiden Siber;
   b. penyampaian informasi Insiden Siber kepada pihak terkait; dan
   c. diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.

6

- Peraturan BSSN 1 tahun 2024

ttg Pengelolaan Insiden Siber



PRESIDEN
REPUBLIK INDONESIA

- 19 -

Pasal 24

(1) Penyelenggara Sistem Elektronik wajib memiliki dan menjalankan prosedur dan sarana untuk pengamanan Sistem Elektronik dalam menghindari gangguan, kegagalan, dan kerugian.

(2) Penyelenggara Sistem Elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian.

(3) Dalam hal terjadi kegagalan atau gangguan sistem yang berdampak serius sebagai akibat perbuatan dari pihak lain terhadap Sistem Elektronik, Penyelenggara Sistem Elektronik wajib mengamankan Informasi Elektronik dan/atau Dokumen Elektronik dan segera melaporkan dalam kesempatan pertama kepada aparat penegak hukum dan Kementerian atau Lembaga terkait.

(4) Ketentuan lebih lanjut mengenai sistem pengamanan sebagaimana dimaksud pada ayat (2) diatur dalam peraturan kepala lembaga yang melaksanakan urusan pemerintahan di bidang keamanan siber.

- PP 71 Tahun 2019

ttg Penyelenggaraan Sistem dan Transaksi Elektronik

Fungsi dan Layanan TTIS

Sumber
Peraturan BSSN No. 1 tahun 2024 tentang Pengelolaan Insiden Siber

LAYANAN UTAMA

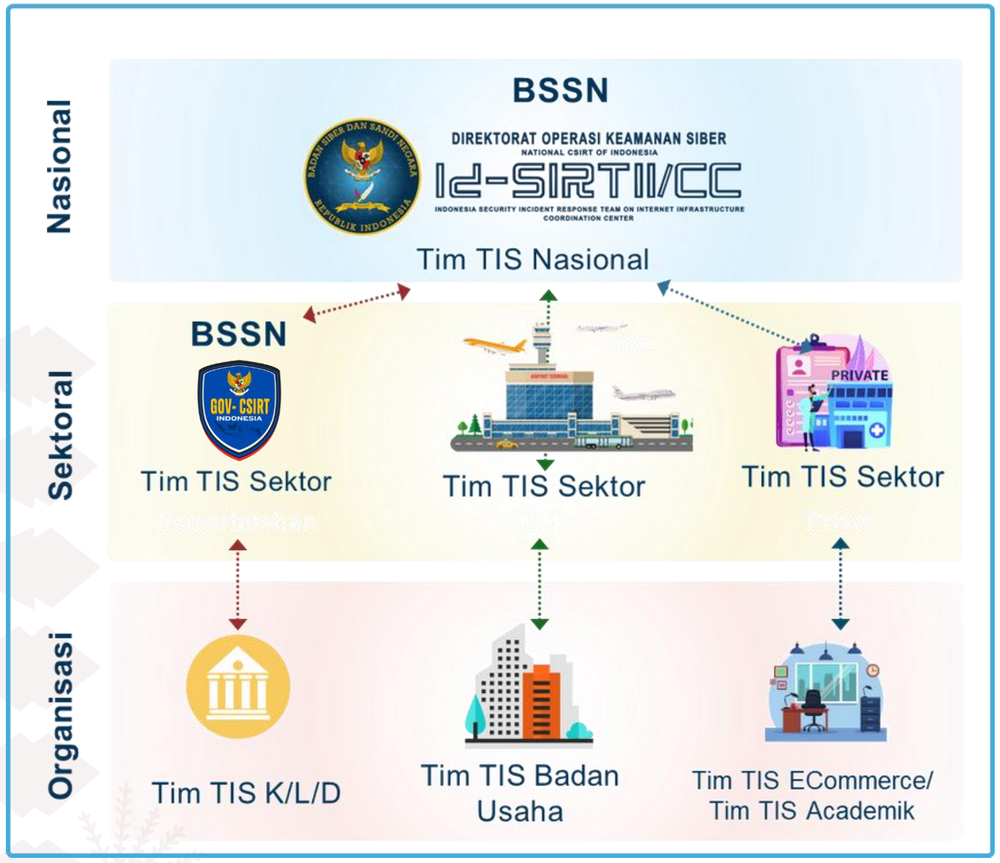
a. *pemberian peringatan terkait Keamanan Siber;*
b. *perumusan panduan teknis penanganan Insiden Siber;*
c. *pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;*
d. *pemilahan (triage) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani; dan*
e. *penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan*
f. *diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber*

LAYANAN LAINNYA

a. *penanganan kerentanan Sistem Elektronik;*
b. *penanganan artefak digital;*
c. *pemberitahuan hasil pengamatan potensi ancaman;*
d. *pendeteksian serangan;*
e. *analisis risiko Keamanan Siber;*
f. *konsultasi terkait kesiapan penanganan Insiden Siber; dan/atau*
g. *pembangunan kesadaran dan kepedulian terhadap Keamanan Siber*

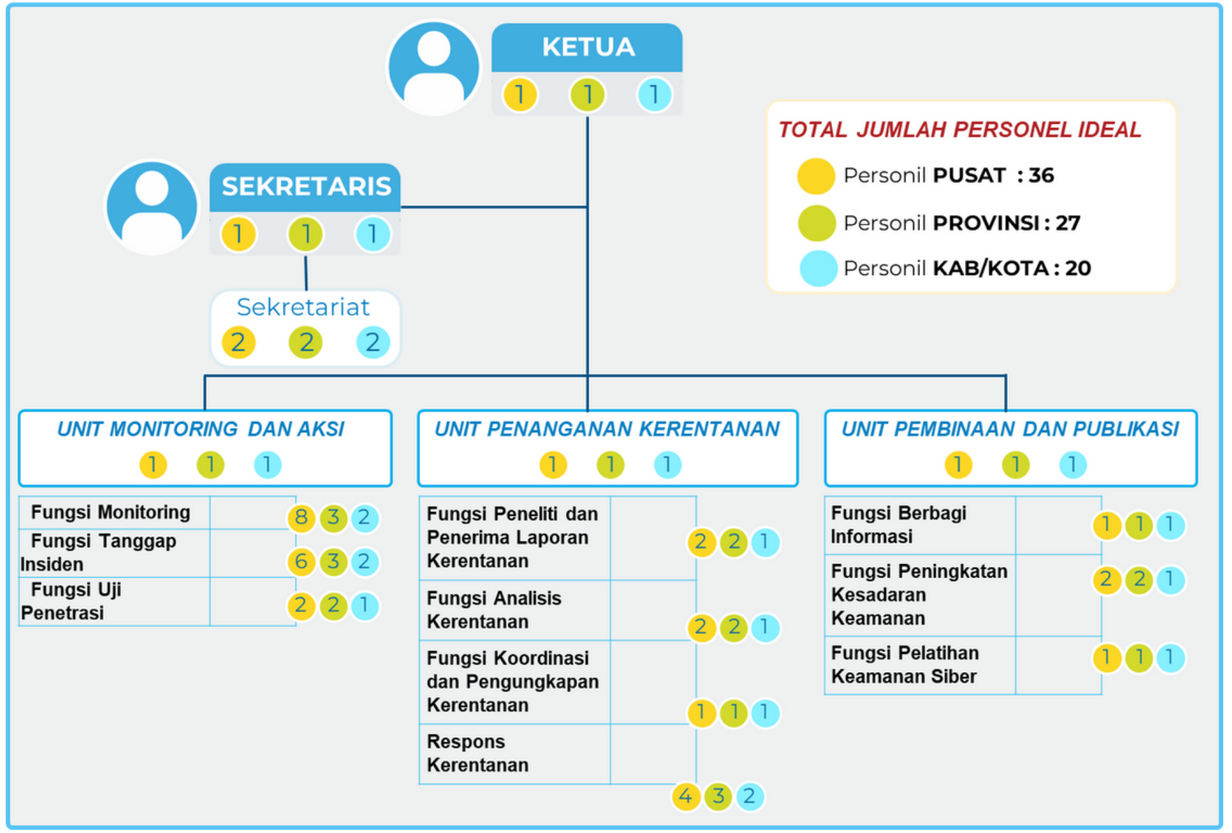
Pola Koordinasi TTIS/CSIRT

Hirarki Tim TIS / CSIRT



- Peraturan Presiden Nomor 82 Tahun 2022
- Peraturan BSSN Nomor 1 Tahun 2024

Struktur Tim TIS / CSIRT



Peraturan Deputi III BSSN Nomor 1 Tahun 2024

BADAN SIBER DAN SANDI NEGARA

Gov-CSIRT Indonesia

Keputusan Kepala BSSN Nomor 722 Tahun 2024

Gov-CSIRT merupakan Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan yang mempunyai fungsi melakukan pencegahan, penanggulangan dan pemulihan insiden siber yang terjadi pada sistem elektronik yang dikelola oleh Sektor Administrasi Pemerintah. Selain itu Gov-CSIRT juga berperan dalam penyampaian informasi insiden siber kepada seluruh konstituen Gov-CSIRT serta melakukan diseminasi informasi keamanan siber dalam rangka pencegahan dan mitigasi insiden siber.

Konstituen Gov-CSIRT (per Agustus 2025) terdiri dari 94 TTIS Pemerintah Pusat, 34 TTIS Pemerintah Provinsi dan 224 TTIS Pemerintah Kab/Kota.

Telegram id: @GovCSIRT_ID

Mail to: govcsirt@bssn[.]go[.]id

WhatsApp: +62 85 123 123 940

Website: https[:]//bssn[.]go[.]id/gov-csirt/

Layanan Gov-CSIRT

Layanan Monitoring dan Aksi :

- Menyelenggarakan fungsi monitoring keamanan siber
- Menyelenggarakan fungsi tanggap insiden siber
- Menyelenggarakan fungsi uji penetrasi

Layanan Penanganan Kerentanan :

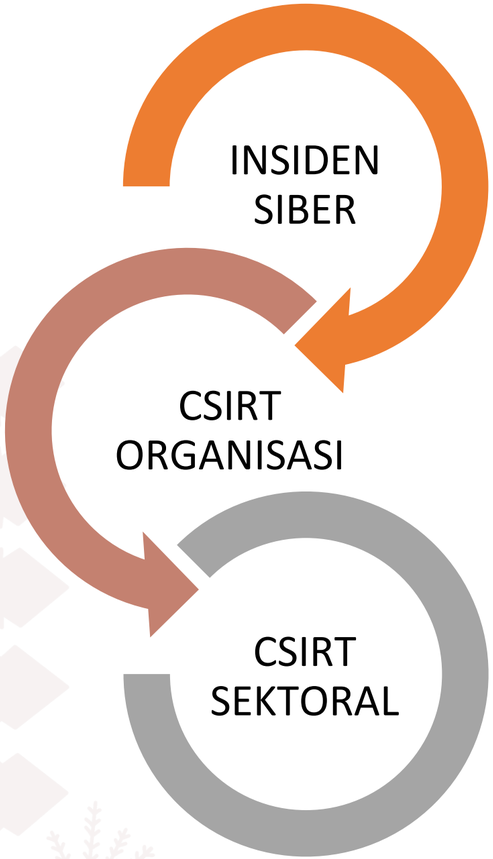
- Menyelenggarakan fungsi peneliti dan penerima laporan kerentanan
- Menyelenggarakan fungsi analisis kerentanan

Layanan Pembinaan dan Publikasi :

- Menyelenggarakan fungsi berbagi informasi
- Menyelenggarakan fungsi peningkatan kesadaran keamanan siber
- Menyelenggarakan fungsi pelatihan keamanan siber

BADAN SIBER DAN SANDI NEGARA

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*

GOV- CSIRT INDONESIA

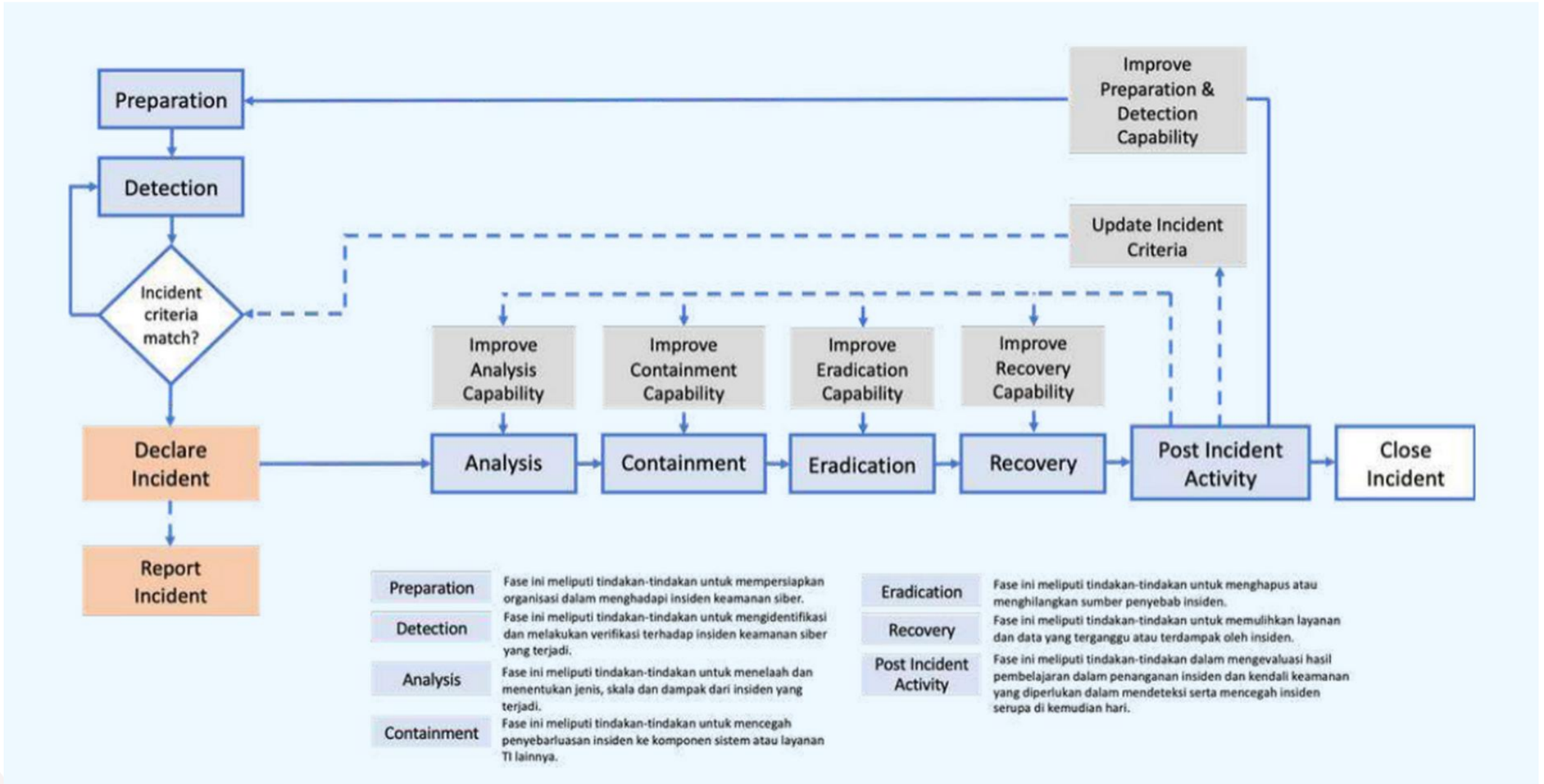
Telegram id: @GovCSIRT_ID

WhatsApp: +62 85 123 123 940

Mail to: govcsirt@bssn[.]go[.]id

Website: https[:]//bssn[.]go[.]id/gov-csirt/

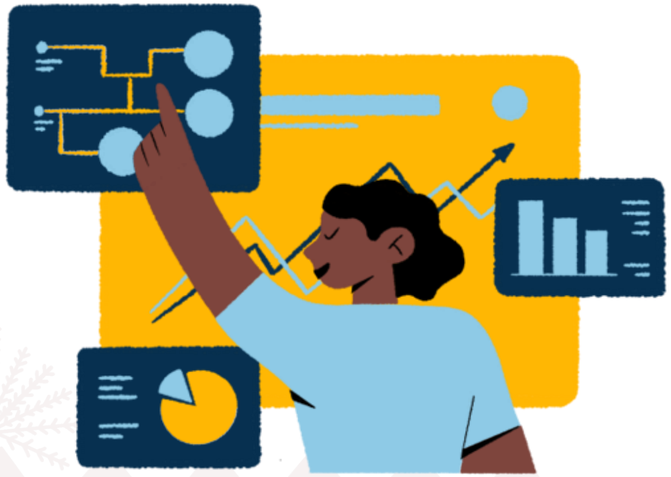
Siklus Pengelolaan Insiden Siber



Fase Analisis

Tujuan Analisis

- Mencari jejak yang ditinggalkan
- Siapa yang melakukan
- Apa yang dilakukan
- Bagaimana dia melakukannya
- Apa yang menjadi target/jalan masuk
- Kapan dilakukannya



Analisis Log: Merekonstruksi kronologi serangan dari catatan aktivitas server.

Analisis File dan Direktori: Mencari jejak dan tools yang ditinggalkan penyerang.

Identifikasi Kerentanan: Menentukan celah keamanan yang dieksploitasi oleh penyerang

Dokumentasi Temuan: Mencatat semua perintah yang dijalankan, temuan, dan waktu kejadian secara rinci untuk laporan.

Fase C-E-R

Rangkaian aksi berurutan untuk menangani insiden secara tuntas: membatasi kerusakan agar tidak meluas, membersihkan ancaman hingga ke akarnya, dan memulihkan sistem kembali ke kondisi operasional yang aman

Containment

Mengisolasi dan menghentikan insiden agar tidak menimbulkan kerusakan lebih lanjut pada sistem lain.

- Memblokir alamat IP penyerang menggunakan firewall
- Melakukan backup atau snapshot sistem yang terinfeksi untuk tujuan analisis forensik dan sebagai bukti insiden

Eradication

Memastikan semua komponen berbahaya dan akar masalah telah dihilangkan sepenuhnya dari sistem.

- Menghapus semua file berbahaya yang ditemukan (webshell, skrip exploit, halaman judi online).
- Menghapus akun pengguna ilegal yang dibuat penyerang
- Menghapus cronjob berbahaya yang ditanam penyerang untuk menjaga persistensi
- Melakukan patching terhadap kerentanan yang dieksploitasi

Recovery

Mengembalikan layanan ke kondisi operasional normal dengan aman dan meminimalkan dampak bagi pengguna.

- Mengembalikan data dari backup terakhir yang diyakini bersih
- Memperbaiki konfigurasi yang salah
- Melakukan hardening (penguatan keamanan) pada sistem sebelum kembali online
- Memonitor sistem secara intensif setelah pulih untuk memastikan penyerang tidak kembali.



“Kechilafan Satu Orang Sahaja
Cukup Sudah Menyebabkan Keruntuhan Negara”

Mayjen TNI (Purn) dr. Roebiono Kertopati
(1914 - 1984)
Bapak Persandian Republik Indonesia

Survey Layanan
D32 BSSN

https://s.id/LayananD32