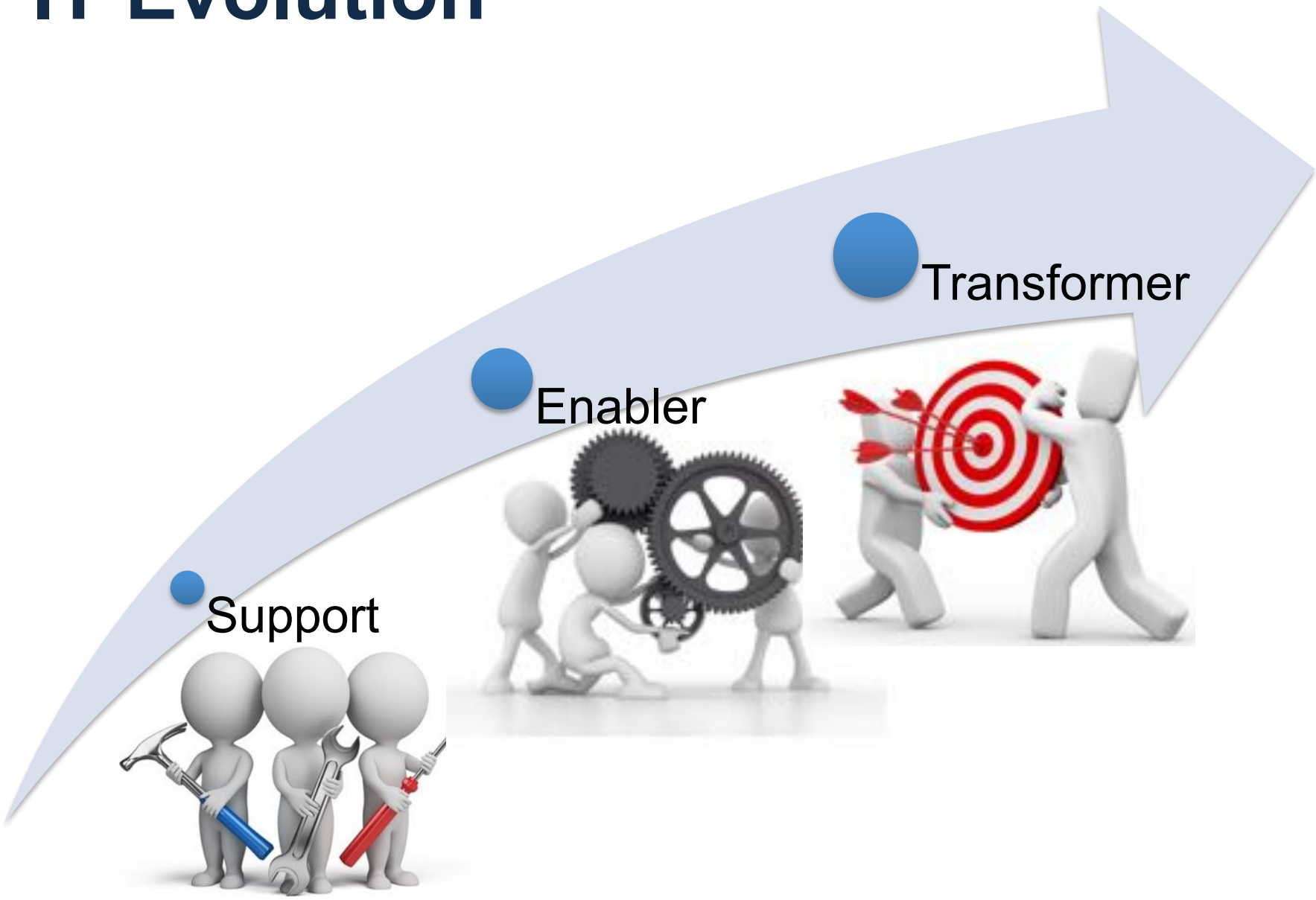
CYBER INCIDENT MANAGEMENT & RESPONSE

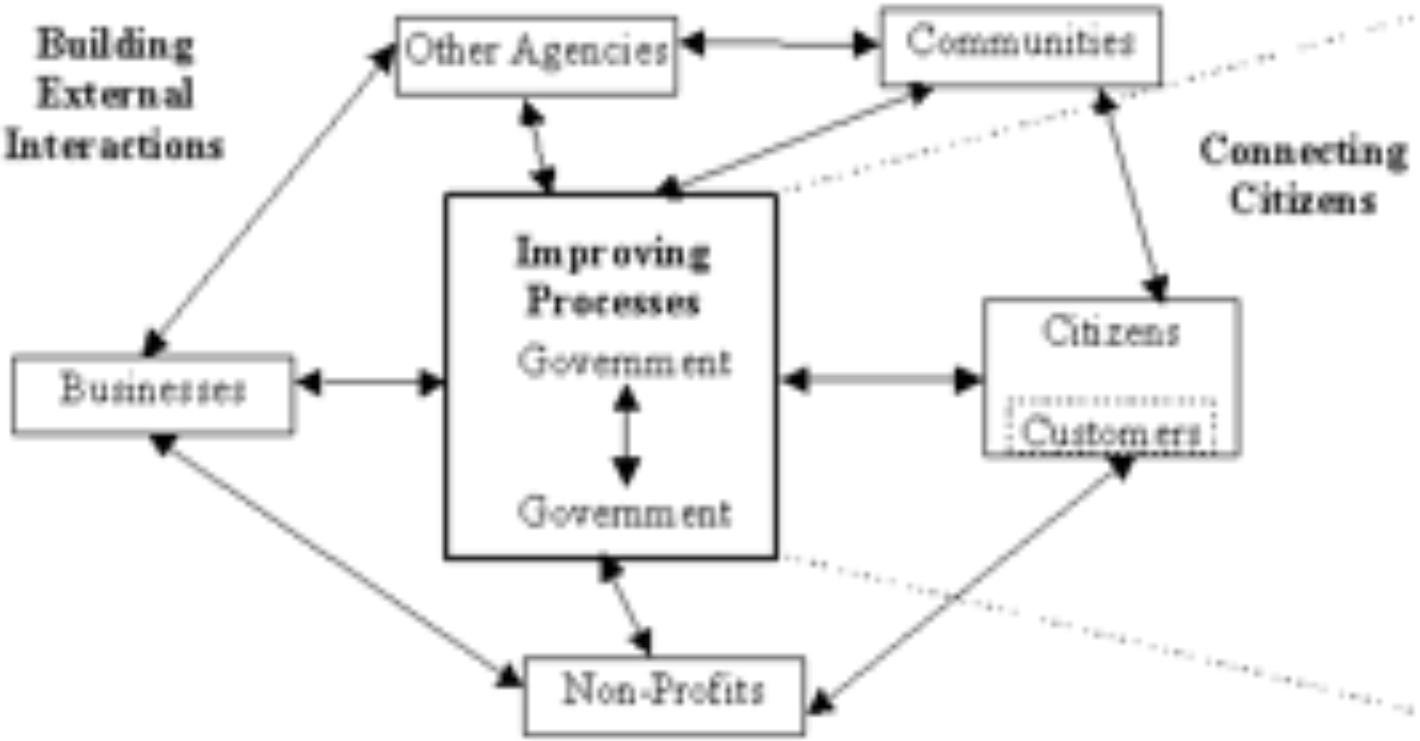
Bisyron Wahyudi

BADAN SIBER & SANDI NEGARA

IT Evolution



Domain eGovernment



Improving government processes: eAdministration
Connecting citizens: eCitizens and eServices
Building external interactions: eSociety

Landasan Hukum eGovernment

- INPRES No.3 Th.2003 tentang Kebijakan dan Strategi Nasional Pengembangan eGov
- UU No.11 Th.2008 tentang Informasi dan Transaksi Elektronik (UU ITE)
- UU No.14 Th.2008 tentang Keterbukaan Informasi Publik (UU KIP)
- PP No. 82 Th. 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

PENYELENGGARAAN SISTEM ELEKTRONIK

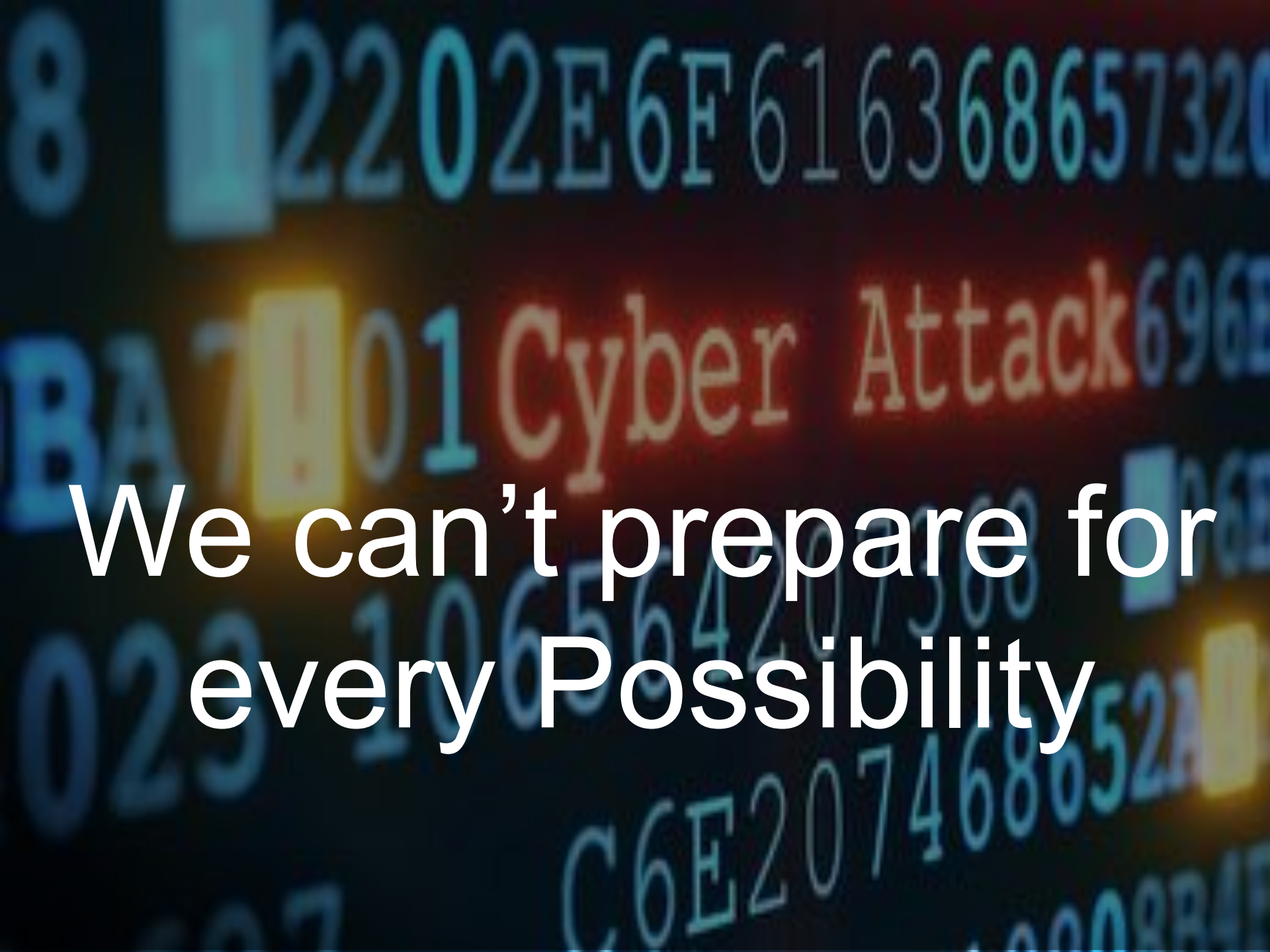
(Pasal 15 dan 16 UU ITE)

- Kewajiban Penyelenggara SistemElektronik:
  (i) keandalan,
  (ii) keamanan,
  (iii) pertanggungjawaban.
- Pengecualian: *force majeure*.
- Persyaratan minimum:
  - dapat menampilkan DE dan/atau IE kembali secara utuh;
  - dapat melindungi keotentikan, integritas, kerahasiaan, ketersediaan, dan keteraksesan;
  - memenuhi prosedur;
  - petunjuk yang cukup.

Sistem Elektronik Strategis

- Yang dimaksud dengan **Sistem Elektronik yang bersifat strategis** adalah Sistem Elektronik yang dapat berdampak serius terhadap **kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara**
- Contoh: sistem elektronik pada sektor kesehatan, perbankan, keuangan, transportasi, perdagangan, telekomunikasi, energi, pertahanan.
- Dilakukan terhadap komponen atau sebagian komponen dalam sistem elektronik sesuai dengan **karakteristik kebutuhan perlindungan** dan **sifat strategisnya**

(penjelasan Pasal 11 PP PSTE)


We can’t prepare for every Possibility

Incident

- Insiden adalah:
  - Kejadian tak terduga yang menyebabkan gangguan operasi normal
- Insiden Keamanan
  - Suatu kejadian pelanggaran terhadap kebijakan keamanan (security policy)
  - Akses secara tidak sah terhadap sistem atau informasi
  - Suatu peristiwa yang menghalangi/mengganggu akses yang sah terhadapa sistem atau informasi


INDONESIA SUMBER SERANGAN TERBANYAK
15,483 TOTAL INSIDEN WEBSITE
DOMAIN TERBANYAK DISERANG: GO.ID
2,260 LAPORAN PENGADUAN PUBLIK
36,423,773 TOTAL AKTIVITAS MALWARE
INDONESIA TARGET SERANGAN TERBANYAK
98,787 TOTAL INFORMASI CELAH KEAMANAN
PORT TERBANYAK DISERANG: 53
205,502,159
SERANGAN

Kebutuhan Incident Response

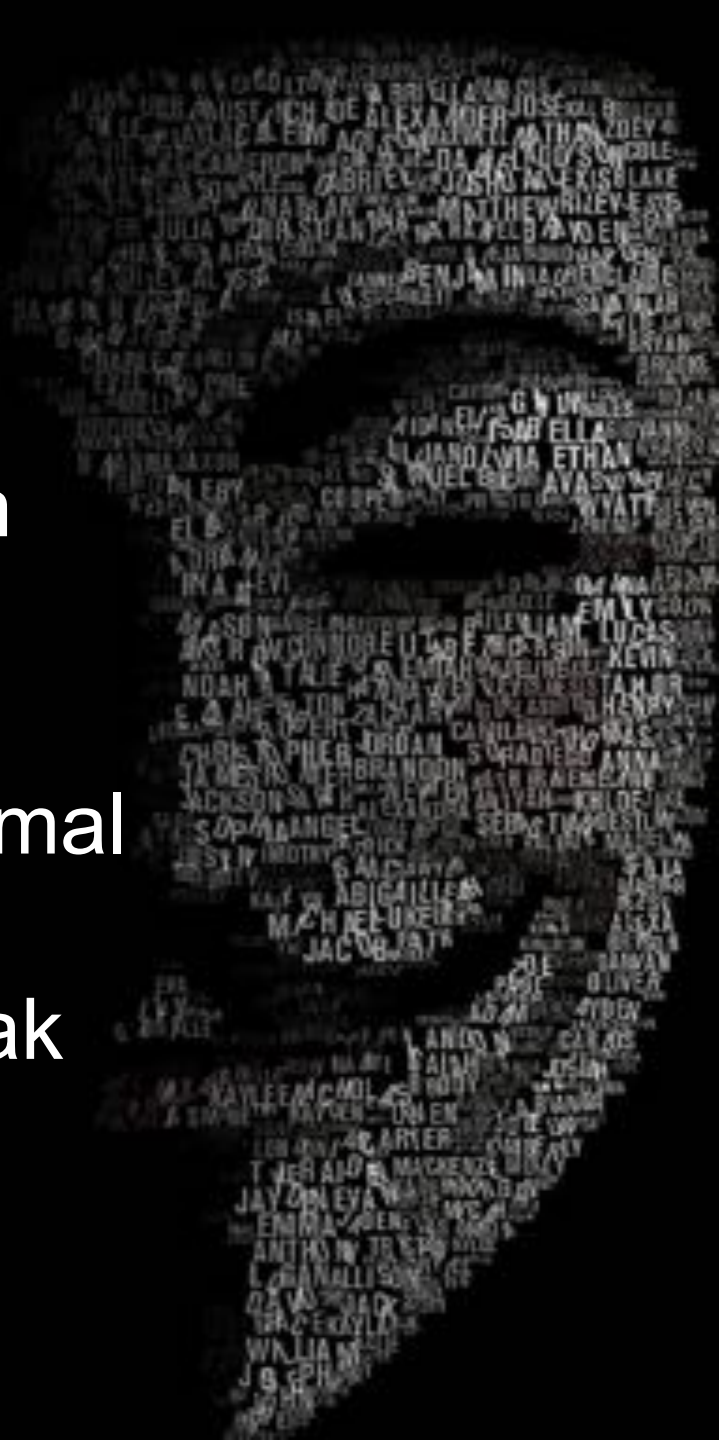
- Serangan baru semakin sering muncul.
- Pencegahan *Risk Assessment* tidak mencegah semua insiden.
- Menangani insiden secara cepat dan sistematis, meminimalkan kerugian.
- Interkoneksi dan Interdependensi system butuh kolaborasi.

Incident Management and Response

- Manajemen insiden mencegah terjadinya insiden
- Aspek operasional dari manajemen risiko
- Tujuannya meminimalkan dan mengelola dampak insiden
- Manajemen risiko dan BIA menentukan prioritas sumber daya
- Perlu Incident Response Program and Planning

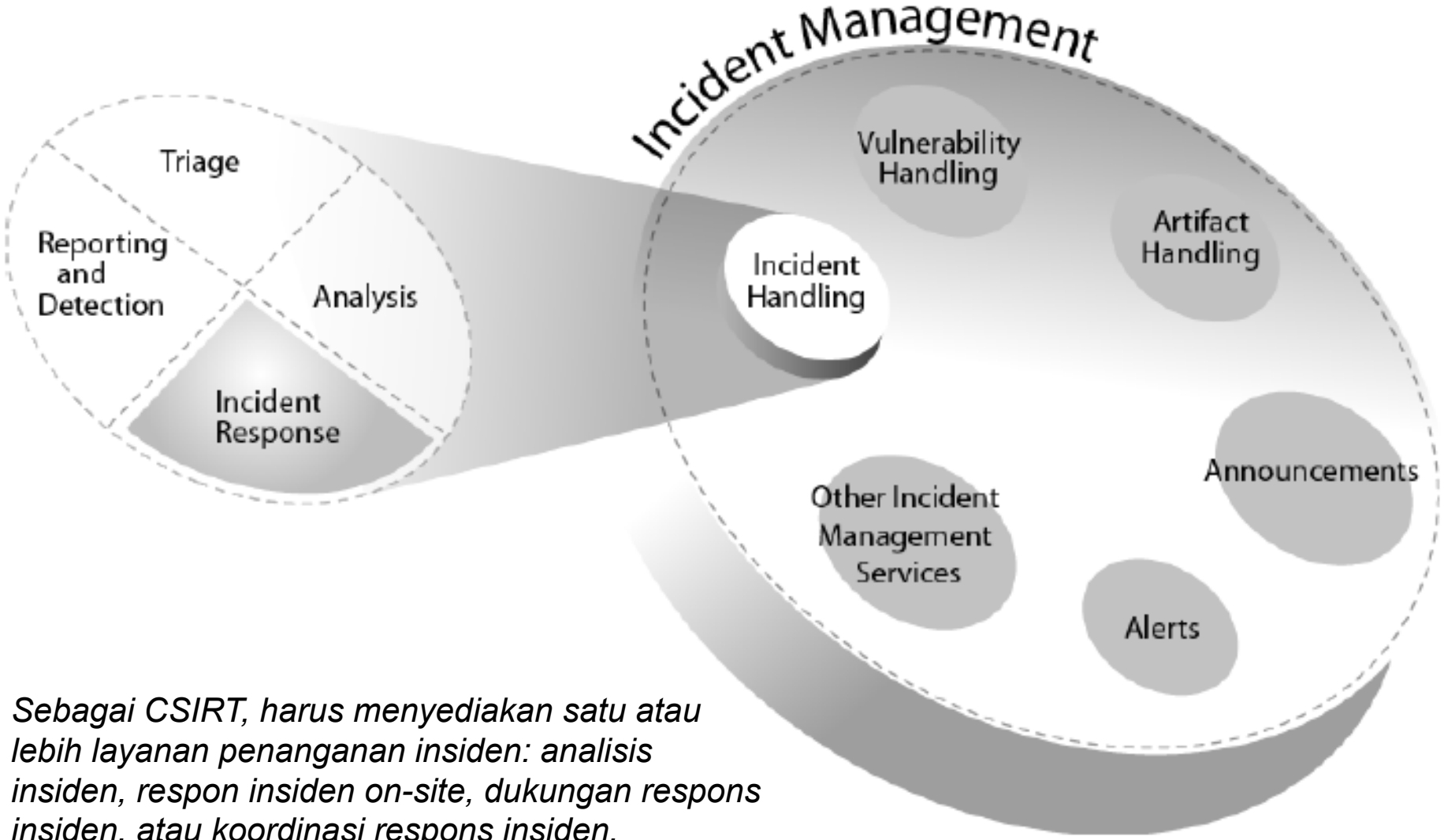
Incident Response

- Deteksi Secepat Mungkin
- Diagnosa Seakurat Mungkin
- Kendalikan Insiden Setepat Mungkin
- Kendalikan Dampak Seminimal Mungkin
- Pulihkan Layanan Terdampak
- Temukan Penyebab Utama
- Cegah Insiden Selanjutnya



- Perlindungan aset informasi penting secara memadai
- Minimalkan risiko ke tingkat yang dapat diterima
- Semua stakeholder memahami IRP dan perannya
- Akar masalah semua insiden ditangani secara memadai
- Dokumentasi dan komunikasi yang lebih baik
- Meningkatnya kesadaran keamanan
- Jaminan kepada semua pihak yang terkena

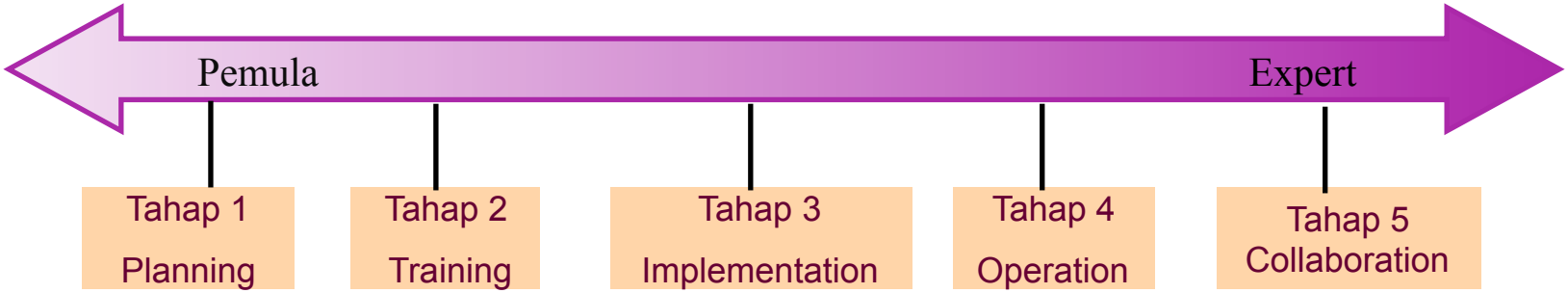
INCIDENT MANAGEMENT



Sebagai CSIRT, harus menyediakan satu atau lebih layanan penanganan insiden: analisis insiden, respon insiden on-site, dukungan respons insiden, atau koordinasi respons insiden.

Tahapan Pembentukan CSIRT

- **Tahap 1 Rencana Startegis**
  - Visi Misi
  - Support dan Sponsorship
  - Stakeholder dan Kunstituen
  - Cakupan dan Tingkat Layanan
- **Tahap 2 Training & Education**
- **Tahap 3 Initial implementation**
  - Kebijakan dan Prosedur
  - Model organisasi, role & responsibility
  - Pengumuman opersional CSIRT
- **Tahap 4 Fase Operasional**
  - Sumberdaya: staff, tools dll.
  - Struktur pelaporan, otoritas
  - Evaluasi kinerja CSIRT
- **Tahap 5 Peer Collaboration**



Incident Response Policy

- Dukungan Pimpinan/Manajemen
- Ruang lingkup dan tujuan dari Respons Insiden
- Mengarahkan Organisasi tim, metode komunikasi, dan bagaimana tim berinteraksi dengan organisasi internal dan eksternal
- Menetapkan apa insiden, dan bagaimana Incident Response Plan and Procedures digunakan
- Persyaratan validasi untuk memastikan kepatuhan dengan semua persyaratan organisasi dan regulasi

Incident Response Procedure

- Menjabarkan proses teknis dan teknik yang digunakan selama investigasi
- Bagian yang paling rinci dan komprehensif dari program Respon Insiden dengan tujuan untuk membangun pendekatan yang sistematis dan konsisten untuk setiap insiden.
- Mungkin dalam bentuk check list, atau formulir atau menguraikan rincian tentang cara menyelidiki ancaman tertentu dan mengumpulkan data log atau bukti untuk keperluan analisis.

Typical IR Procedures

- Komunikasi - baik internal maupun eksternal
- Pemberitahuan Eskalasi
- Formulir Pelacakan Insiden
- Pelaporan dan Dokumentasi Insiden
- Daftar Pemeriksaan Investigasi
- Daftar Periksa Remediasi berdasarkan klasifikasi Risiko dan Ancaman
- Koleksi Bukti dan Penanganan “Chain of Custody”
- Investigasi dan Dokumentasi Forensik
- Retensi dan Penghancuran Data
- Perjanjian Non-Disclosure

Incident Response Plan

- Tentukan apa insiden itu (*taksonomi insiden, identifikasi dan remediasi serangan, dan kerangka klasifikasi-data*)
- Mengatasi masalah organisasi dan menetapkan peran (*peran dan tanggung jawab yang ditentukan dengan jelas*)
- Identitas departemen terkait dan melibatkan mereka
- Identifikasi KPI untuk mengukur kinerja (*waktu untuk mendeteksi, laporkan insiden, triase dan penyelidikan*)
- Tes / Evaluasi / Latihan IRP
- Tinjau/Review IRP secara berkala
- Bentuk tim respon insiden (CSIRT)
- Menerapkan perangkat dan sumber daya yang tepat
- Menetapkan strategi komunikasi
- Menunjuk Point of Contact (POC)

Tugas POC

- Menerima dan menanggapi laporan insiden keamanan siber
- Menerima dukungan dan saran dalam menanggapi dan memitigasi insiden siber
- Memonitor insiden keamanan atau serangan siber
- Memberikan saran dan peringatan kepada stakeholder dan konstituen untuk meningkatkan ketahanan keamanan siber
- Sebagai kontak terpercaya (*trusted*) untuk *sharing information*

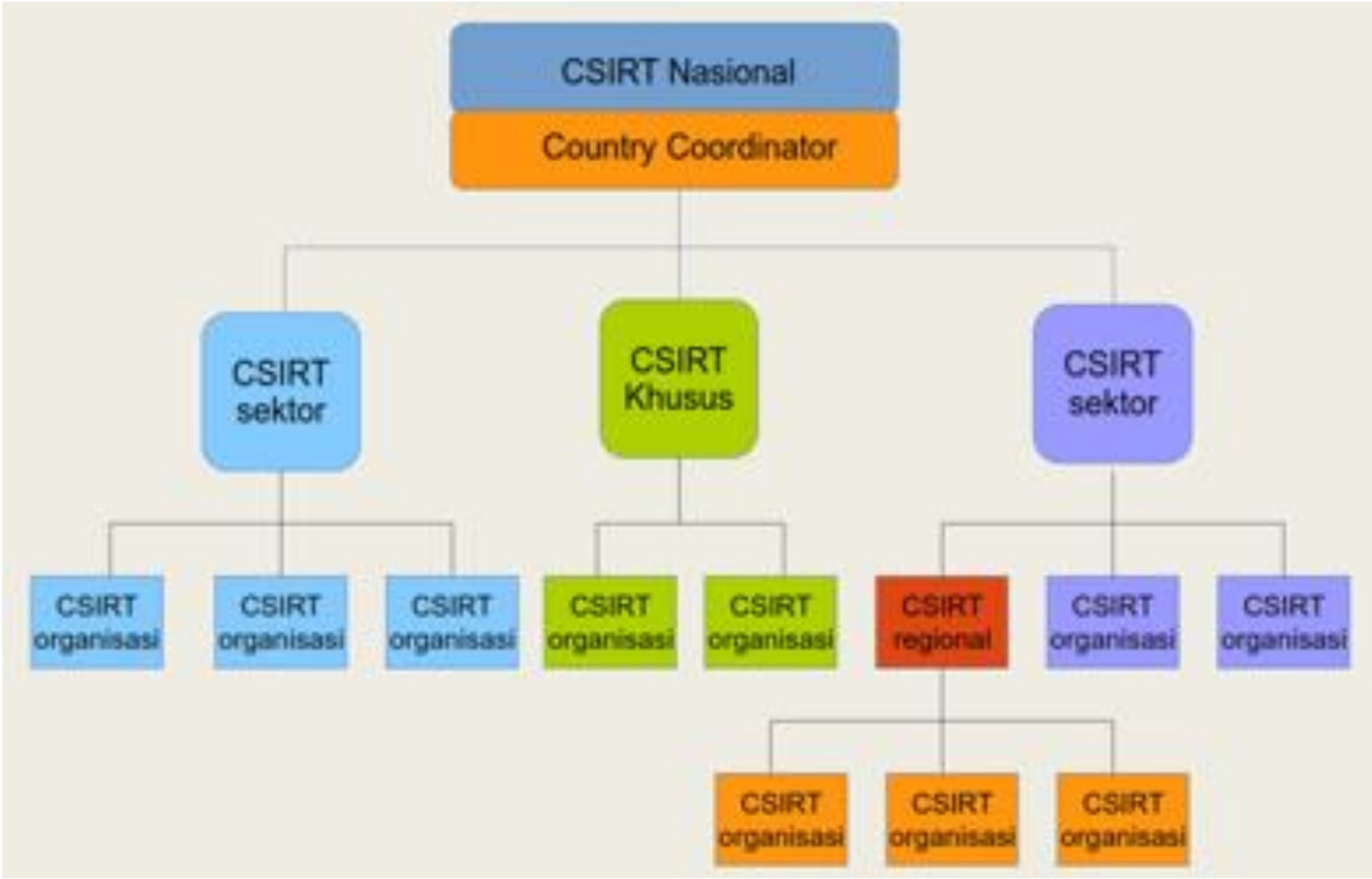
Team Structure Model

Central Incident Response Team

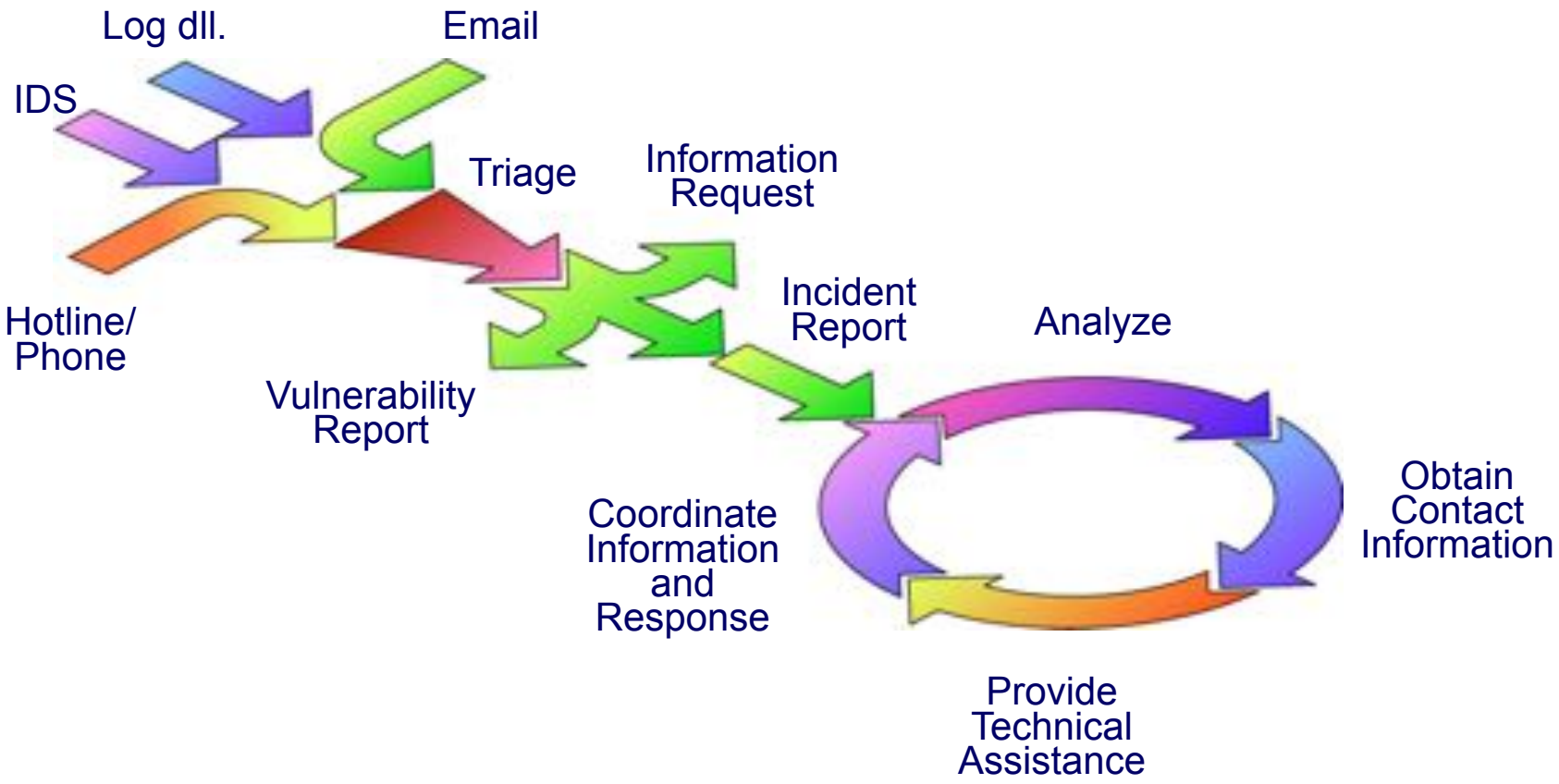
Distributed Incident Response Team

Coordinating Team

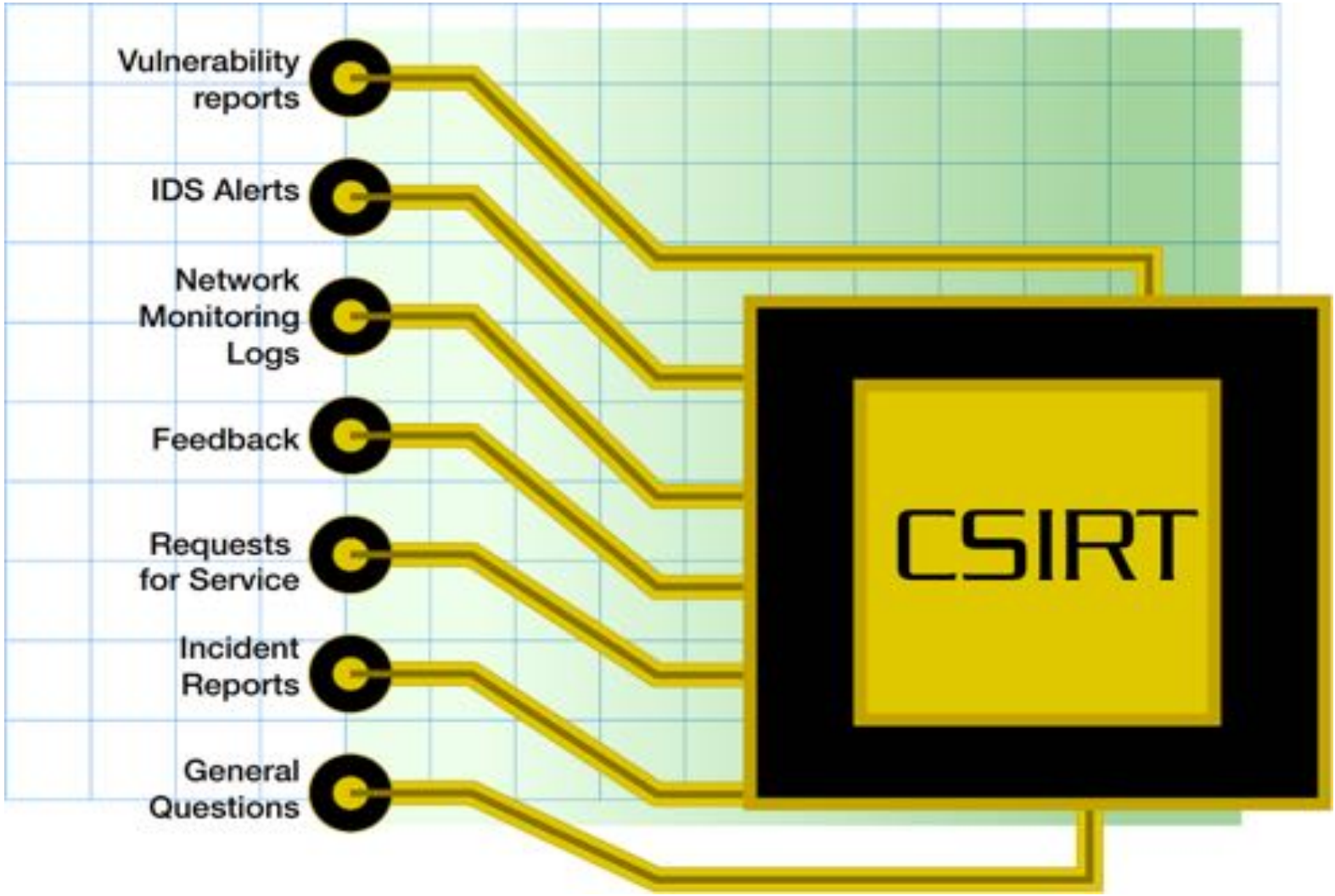
Struktur CSIRT



Incident Handling Life Cycle



Apa saja yang dilaporkan?



ALUR ADUAN
INSIDEN SIBER

Segera laporkan !!!

apabila anda menemukan insiden siber

Terjadi
insiden siber

Kumpulkan bukti insiden berupa foto / screenshot insiden / log file yang ditemukan

BADAN SIBER DAN SANDI NEGARA
BSSN

Aduan segera kami tangani

Hubungi (021) 78833610
Laporkan & Kirimkan bukti ke
bantuan70@bssn.go.id atau
pusopskamsinas@bssn.go.id

PUSAT KONTAK SIBER

Pusat Operasi Keamanan Siber Nasional BSSN

Kesimpulan

- Perlu dibentuk Tim Respon Insiden di tiap Instansi Pemerintah Pusat dan Daerah.
- Tim perlu dukungan penuh pimpinan / organisasi
- SDM perlu Training terkait Penanganan insiden
- Kepala Pusat Data/Kepala Dinas Kominfo sebagai Ketua CSIRT?
- Perlu PoC (*Point of Contact*) untuk kemudahan komunikasi dan koordinasi
- Perlu forum komunikasi antar csirt untuk bertukar informasi (*information sharing*)