BADAN SIBER & SANDI NEGARA

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

DIREKTORAT PENANGGULANGAN DAN PEMULIHAN PEMERINTAH,
DEPUTI BIDANG PENANGGULANGAN DAN PEMULIHAN
BSSN

PENGGUNA INTERNET DI INDONESIA

Pengguna Internet di Indonesia :
Tahun 2018 : 143,26 Juta Jiwa
Tahun 2019 : 171,17 Juta Jiwa

Prosentasi Pengguna Internet di Indonesia Tahun 2018 sebanyak
64,8% dari Jumlah Populasi Masyarakat Indonesia.

Terjadi Kenaikan jumlah Pengguna Internet di Indonesia sebesar
10,12 % (dalam 1 Tahun)

Sumber : Hasil Survey Asosiasi Penyelenggara Internet Indonesia (APJII) 2018

BADAN SIBER & SANDI NEGARA

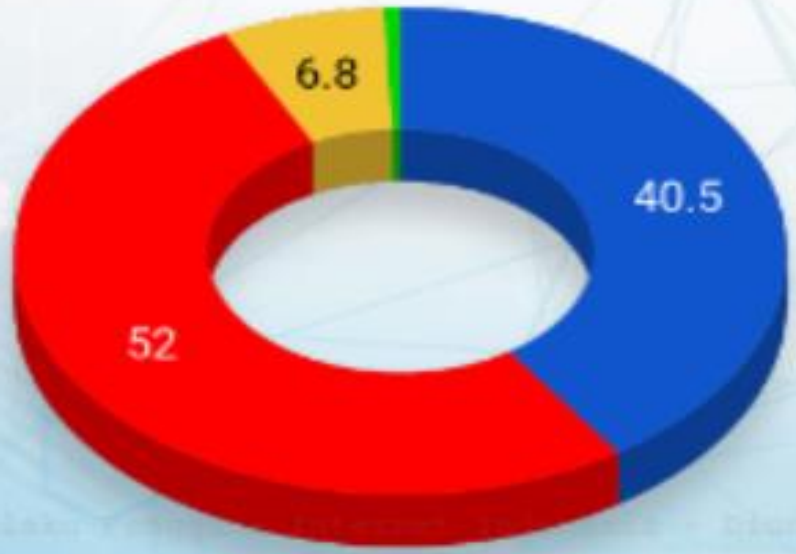
INFOGRAFIS

HASIL SURVEI 2018

POLLING INDONESIA

APJII Asosiasi Penyelenggara Jasa Internet Indonesia

Sampai saat ini, apakah pernah atau tidak pernah perangkat anda untuk terkoneksi dengan internet terkena virus?



- Ya, Pernah
- Tidak Pernah
- Tidak Tahu
- Tidak Jawab

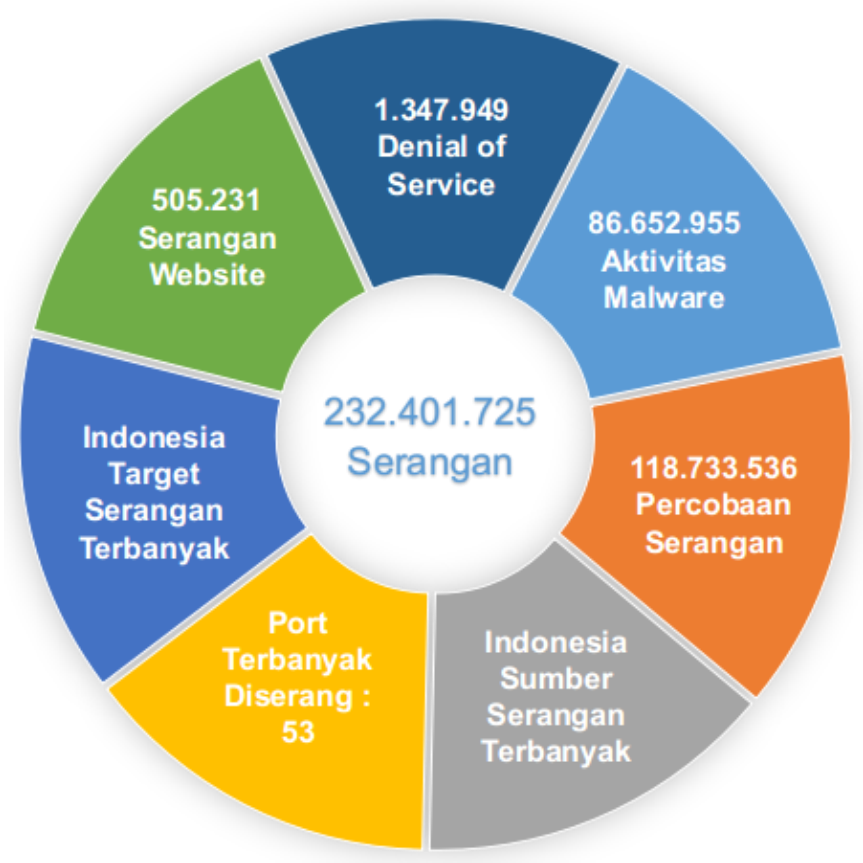
Sumber : Hasil Survey Asosiasi Penyelenggara Internet Indonesia (APJII) 2018

BADAN SIBER & SANDI NEGARA

Sumber : Hasil Survey Asosiasi Penyelenggara Internet Indonesia (APJII) 2018

BADAN SIBER & SANDI NEGARA

DATA SERANGAN SIBER DI INDONESIA



Sumber : BSSN

- Indonesia menjadi Target Serangan dan Sumber Serangan Terbanyak
- Jumlah IP Indonesia yang terinfeksi botnet mencapai 15 Juta IP

BADAN SIBER &
SANDI NEGARA

INSIDEN KEAMANAN SIBER

- Insiden adalah :

  Kejadian tak terduga yang menyebabkan gangguan operasi normal

- Keamanan Siber merupakan :

  terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), nir-sangkal (*non-repudiation*), otentisitas (*authentication*), akuntabilitas (*accountability*) dan keandalan (*reliability*) layanan dalam domain siber

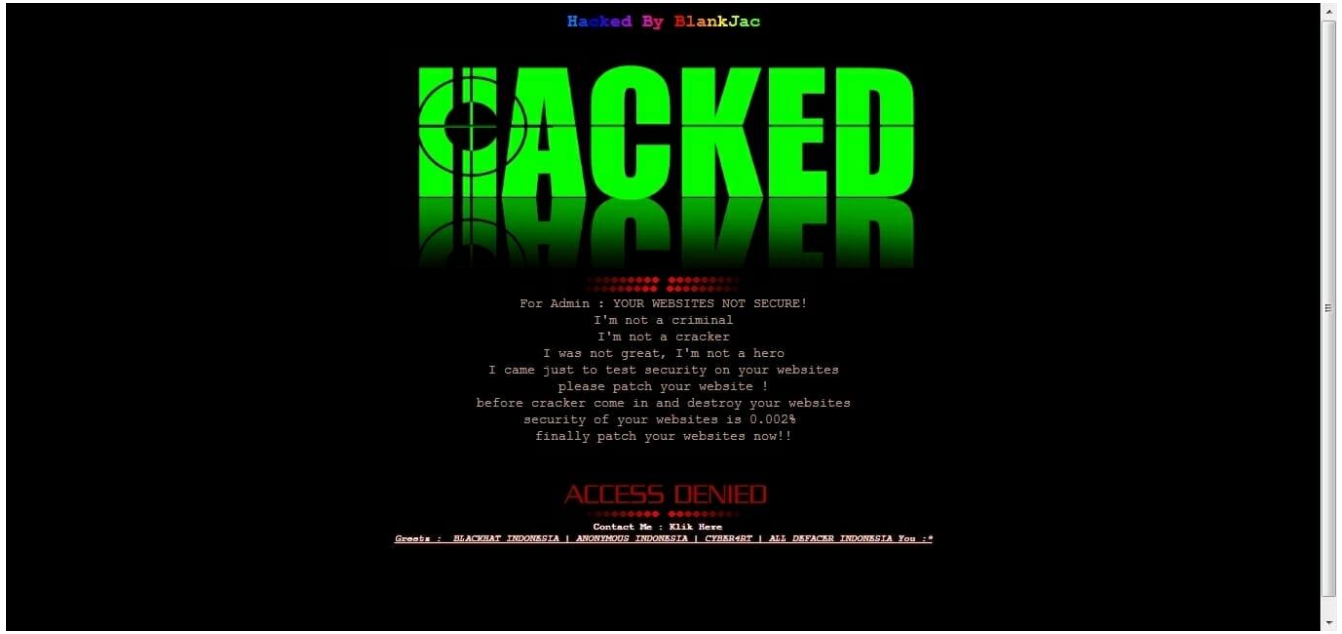
- Insiden Keamanan Siber merupakan :
  - kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik atau Infrastruktur Informasi Kritikal bagi layanan publik dan atau;
  - pelanggaran kepatuhan terhadap kebijakan keamanan siber

BADAN SIBER & SANDI NEGARA

CONTOH JENIS INSIDEN KEAMANAN SIBER

- **Web Defacement**

Tindakan merubah tampilan suatu website baik itu halaman utama, index file, atau pun halaman lain yang masih terikat dalam satu url dengan website tersebut

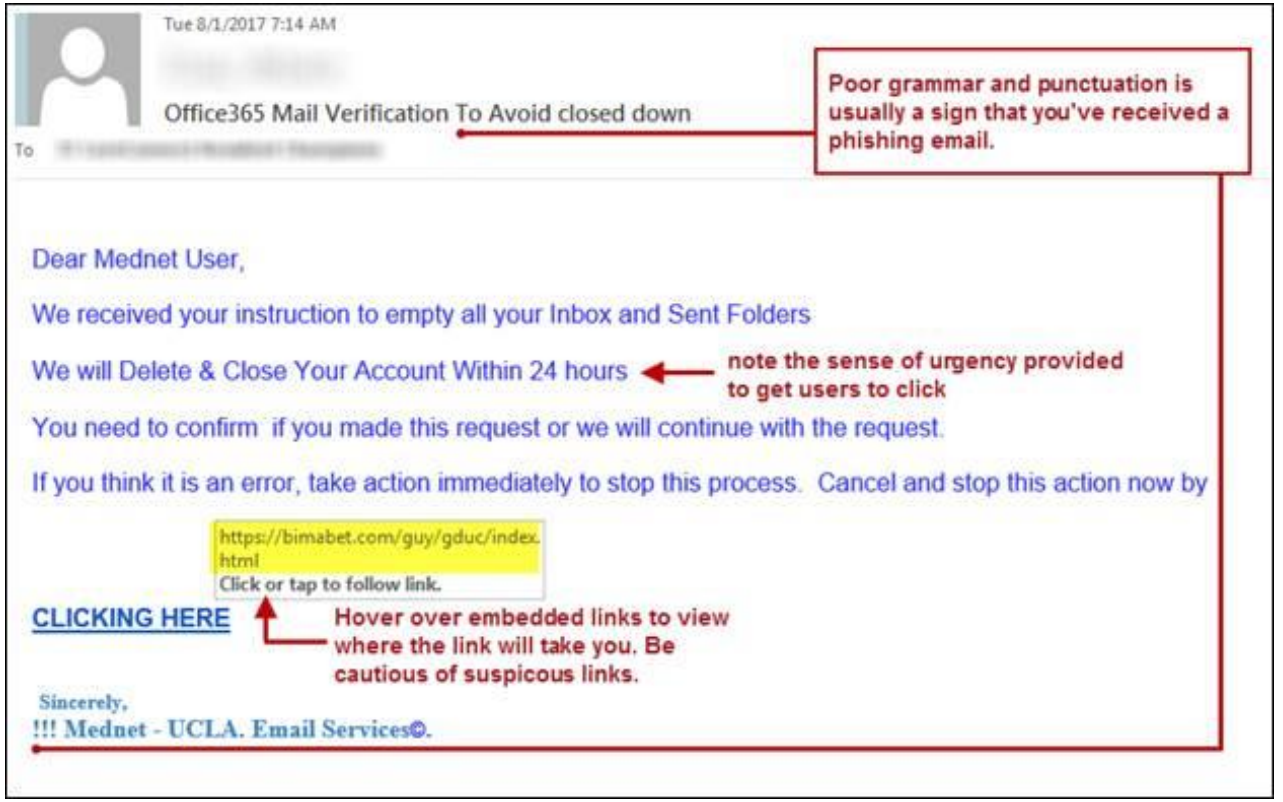


BADAN SIBER & SANDI NEGARA

CONTOH JENIS INSIDEN KEAMANAN SIBER

- **Phising**

Tindakan memperoleh informasi pribadi seperti User ID, Password dan data-data sensitif lainnya dengan menyamar sebagai orang atau organisasi yang berwenang melalui sebuah email



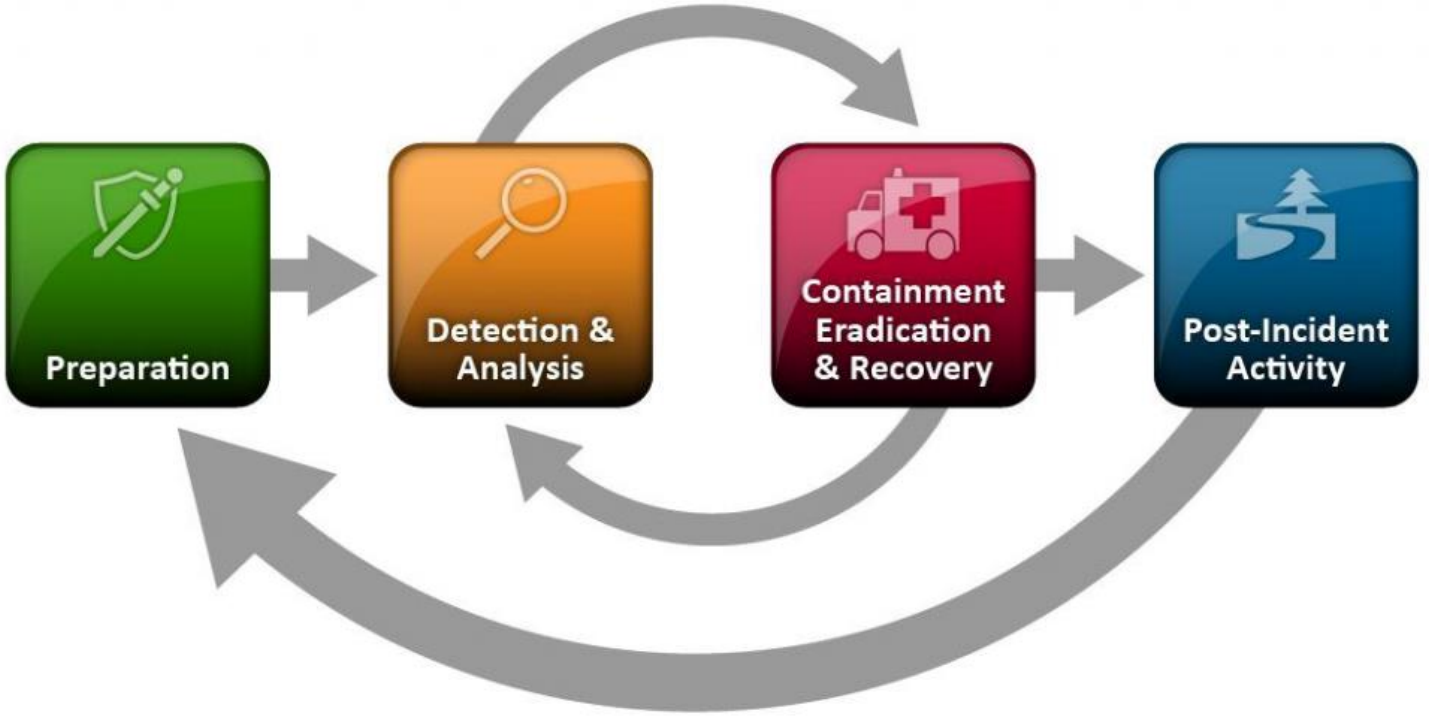
BADAN SIBER & SANDI NEGARA

CONTOH JENIS INSIDEN KEAMANAN SIBER

- **Ransomware**

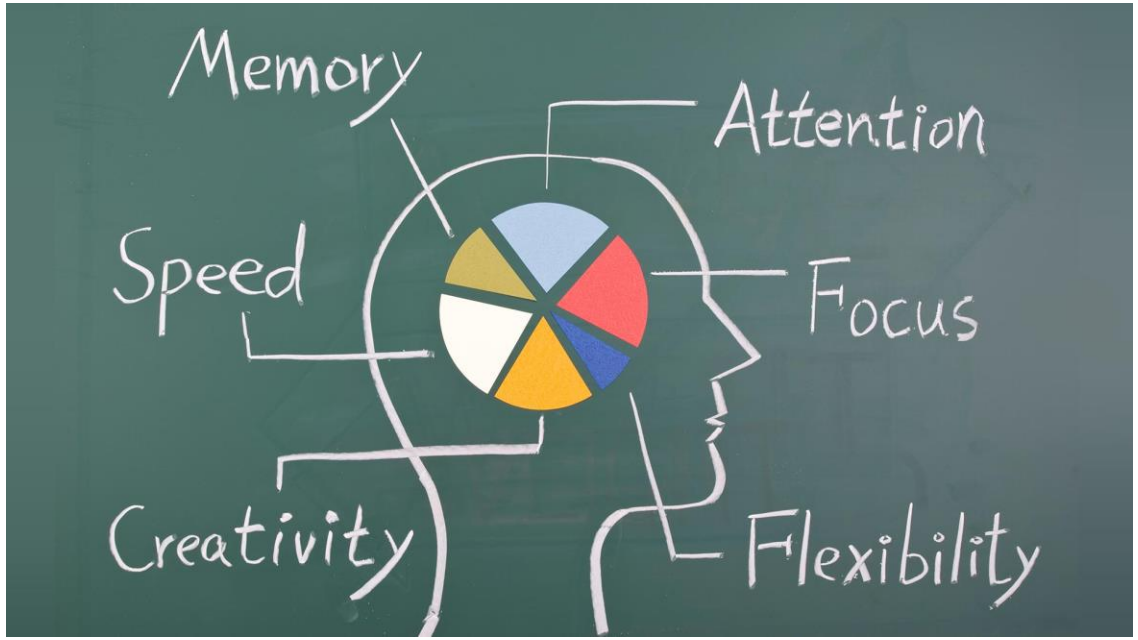
Suatu *malware* yang mampu mengambil alih kendali atas sebuah komputer dan mencegah penggunanya untuk mengakses data hingga tebusan dibayar.

SIKLUS RESPON INSIDEN



PREPARATION

- Komunikasi
- Jenis Insiden
- Tim Perespon Insiden
- Rencana dan Strategi Respon Insiden
- Tools Respon Insiden
- Dokumen Penanganan Insiden



DETECTION AND ANALYSIS

- Bukti Insiden
- Topologi Jaringan dan Sistem Komputer
- Kebijakan Keamanan (Security Policy)
- Dampak dan Keparahan Insiden *(Impact and Severity of Incident)*

BADAN SIBER & SANDI NEGARA

CONTAINMENT, ERADICATION AND RECOVERY

- Lokalisir sistem terdampak
- Penghapusan artifak
- Perbaikan sistem terdampak
- Pemulihan

POST-INCIDENT

- Lesson-Learned
- Vulnerability Assessment
- Hardening

BADAN SIBER & SANDI NEGARA

SEJARAH CSIRT

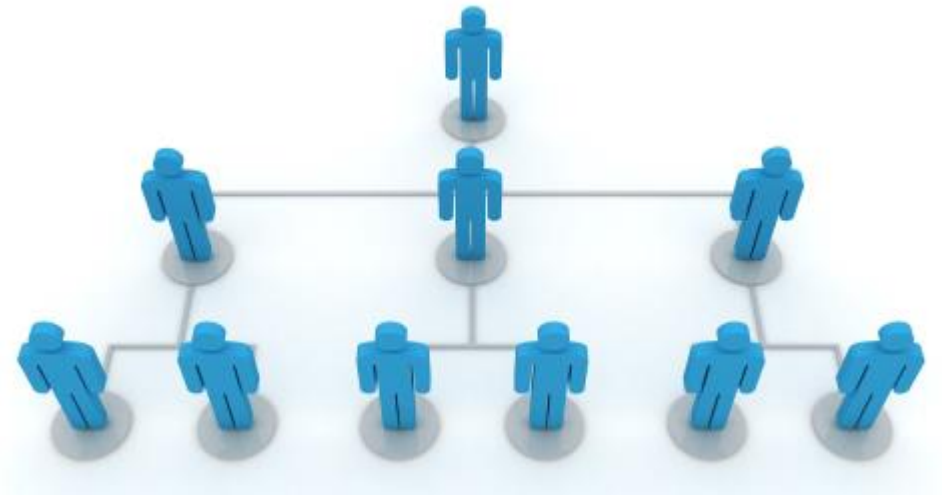
Diawali dengan terjadinya wabah "*worm*" yang bernama "*Moris worm*". "*worm*" ini menyebar dan menginfeksi Sistem dan Infrastruktur TI dunia pada tahun 1980-an. Oleh karenanya, maka DARPA (Defence Advanced Research Project Agency) membentuk SEI (Software Engineering Institute) dan kemudian membentuk CERT/CC (Computer Emergency Response Team/Coordination Center) di Carnegie Melon University (CMU) untuk menangani segala insiden pada computer termasuk wabah "worm".

Model ini segera diadopsi di Eropa, dan 1992, SURFnet meluncurkan CSIRT pertama di Eropa, bernama SURFnet-CERT. Seiring berjalannya waktu, CERT mengalami pengembangan layanan yang meliputi *Alert*, *Security Advisory*, *training* dan lainnya. Hingga akhirnya pada tahun 1998 masyarakat internet dunia dibawah IETF/ICANN menyepakati pembentukan CSIRT.

DIMANA CSIRT DITEMPATKAN ?

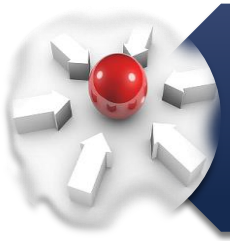
Tidak ada Standar tentang Lokasi CSIRT Organisasi harus berada di dalam sebuah divisi tertentu.

CSIRT merupakan bagian dari Penyelenggaraan **Keamanan Informasi** dan **Teknologi Informasi Komunikasi (TIK)** **sehingga CSIRT dilaksanakan oleh Unit Kerja yang memiliki kewenangan di bidang tersebut.**



BADAN SIBER & SANDI NEGARA

MODEL CSIRT



Tim Penanggulangan Insiden sentral

Tim Penanggulangan Insiden Terdistribusi

Tim Koordinasi

Organisasi memiliki Tim Penanganan Internal

Organisasi tidak perlu memiliki Tim Penanganan Internal

BADAN SIBER & SANDI NEGARA

PERTIMBANGAN PEMILIHAN MODEL CSIRT

- Full-time vs Part-time

  Idealnya Tim Penanganan Insiden bekerja Full-time 24/7. Namun jika staf terbatas, maka pemilihan *part time* dibolehkan dengan catatan ketika keadaan darurat terjadi, anggota tim dapat dihubungi dengan cepat, dan mereka dapat membantu melakukan penanganan insiden saat itu juga.

- Keahlian Staf

  Keahlian dan pengalaman khusus dalam menangani insiden merupakan hal yang penting untuk dimiliki oleh Tim CSIRT jika Sebuah Organisasi tersebut memilih untuk menangani insiden secara mandiri. Namun kebutuhan keahlian khusus menangani insiden dapat diabaikan jika model "Tim Koordinasi" yang dipilih oleh Organisasi.

- Biaya

  Faktor utama sebuah CSIRT dapat bekerja secara efektif. Kebutuhan biaya berbanding lurus dengan jumlah layanan CSIRT yang ditawarkan kepada konstituen dan Kompleksitas pekerjaan Model CSIRT yang dipilih.

PERTIMBANGAN KEBUTUHAN JUMLAH STAFF CSIRT

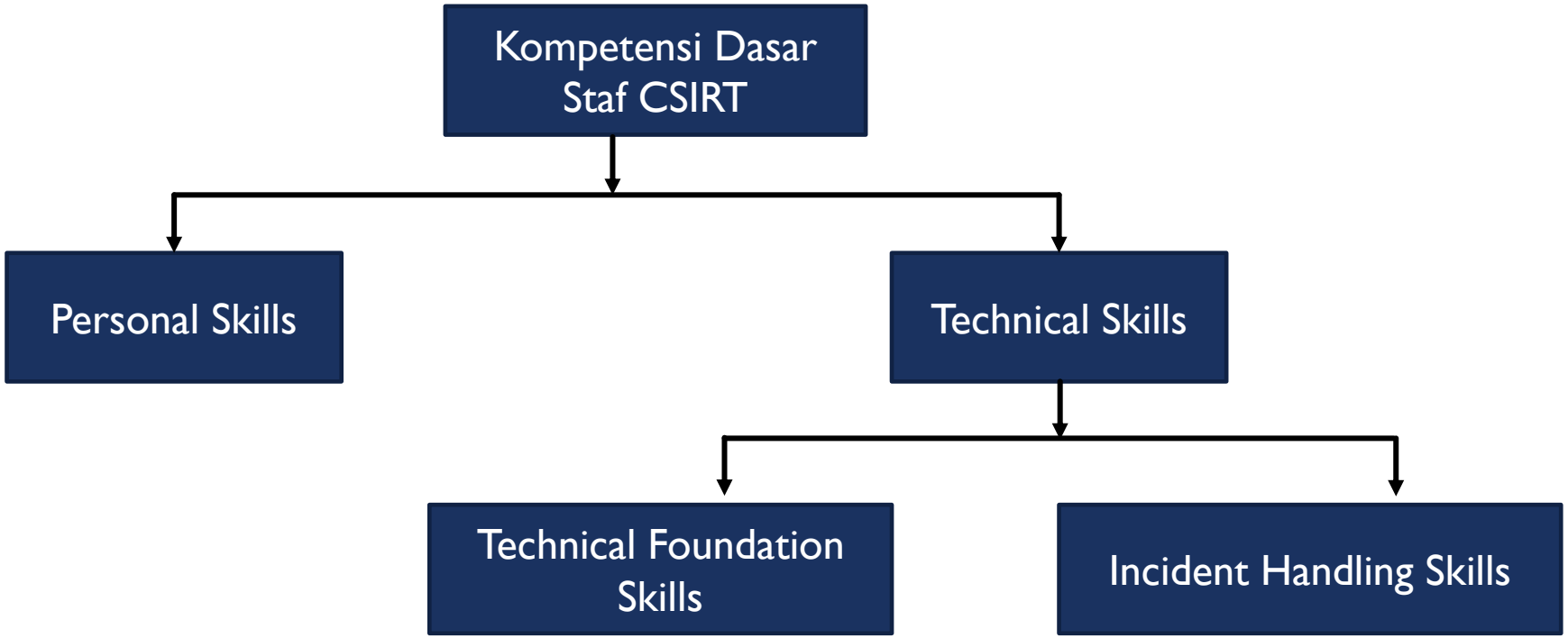
- Model CSIRT yang dipilih

  Jumlah staf CSIRT yang dibutuhkan oleh Organisasi yang mengoperasionalkan sebagai Tim Koordinasi akan leih sedikit jumlah kebutuhan stafnya jika dibanding dengan model CSIRT terpusat atau terdistribusi
- Layanan yang Diberikan

  Kebutuhan jumlah staf sangat dipengaruhi oleh jumlah dan kebutuhan layanan yang diberikan kepada konstituen. Sehingga biaya yang dikeluarkan untuk operasional staff tidak lebih besar dari manfaat yang diterima.
- Seberapa Besar dan Kondisi Geografis Target Konstituen

  Semakin besar jumlah konstituen dan kondisi geografis maka semakin besar jumlah staf yang dibutuhkan. Hal ini disebabkan oleh ketersediaan dan kecepatan staf dalam penanganan insiden akan mengurangi potensi kerusakan dan kerugian yang diakibatkan oleh sebuah Insiden.

KOMPETENSI STAFF CSIRT



PERSONAL SKILL

- Communication ✓
- Presentation Skills
- Diplomacy
- Ability to Follow Policies and Procedures ✓
- Team Skills
- Integrity ✓
- Knowing One's Limits
- Coping with Stress
- Problem Solving ✓
- Time Management ✓

Standar Kompetensi Staff CSIRT (✓)

Standar Kompetensi tersebut merupakan syarat minimal kompetensi yang harus dimiliki oleh Staff CSIRT

BADAN SIBER & SANDI NEGARA

TECHNICAL FOUNDATION SKILLS

- The Internet ✓
- Security Principles ✓
- Security Vulnerabilities/Weakness ✓
- Risk ✓
- Network Protocol
- Network Applications and Services
- Network Security Issues
- Host/System Security Issues
- Malicious Code ✓
- Programming Skills

Standar Kompetensi Staff CSIRT (✓)

Standar Kompetensi tersebut merupakan syarat minimal kompetensi yang harus dimiliki oleh Staff CSIRT

INCIDENT HANDLING SKILLS

- Local Team Policies and Procedures ✓
- Understanding/Identifying Intruder Techniques ✓
- Incident Analysis ✓
- Maintenance of Incident Records ✓

Standar Kompetensi Staff CSIRT (✓)

Standar Kompetensi tersebut merupakan syarat minimal kompetensi yang harus dimiliki oleh Staff CSIRT

KEBUTUHAN KOMPETENSI STAFF CSIRT

- **CSIRT Koordinasi**

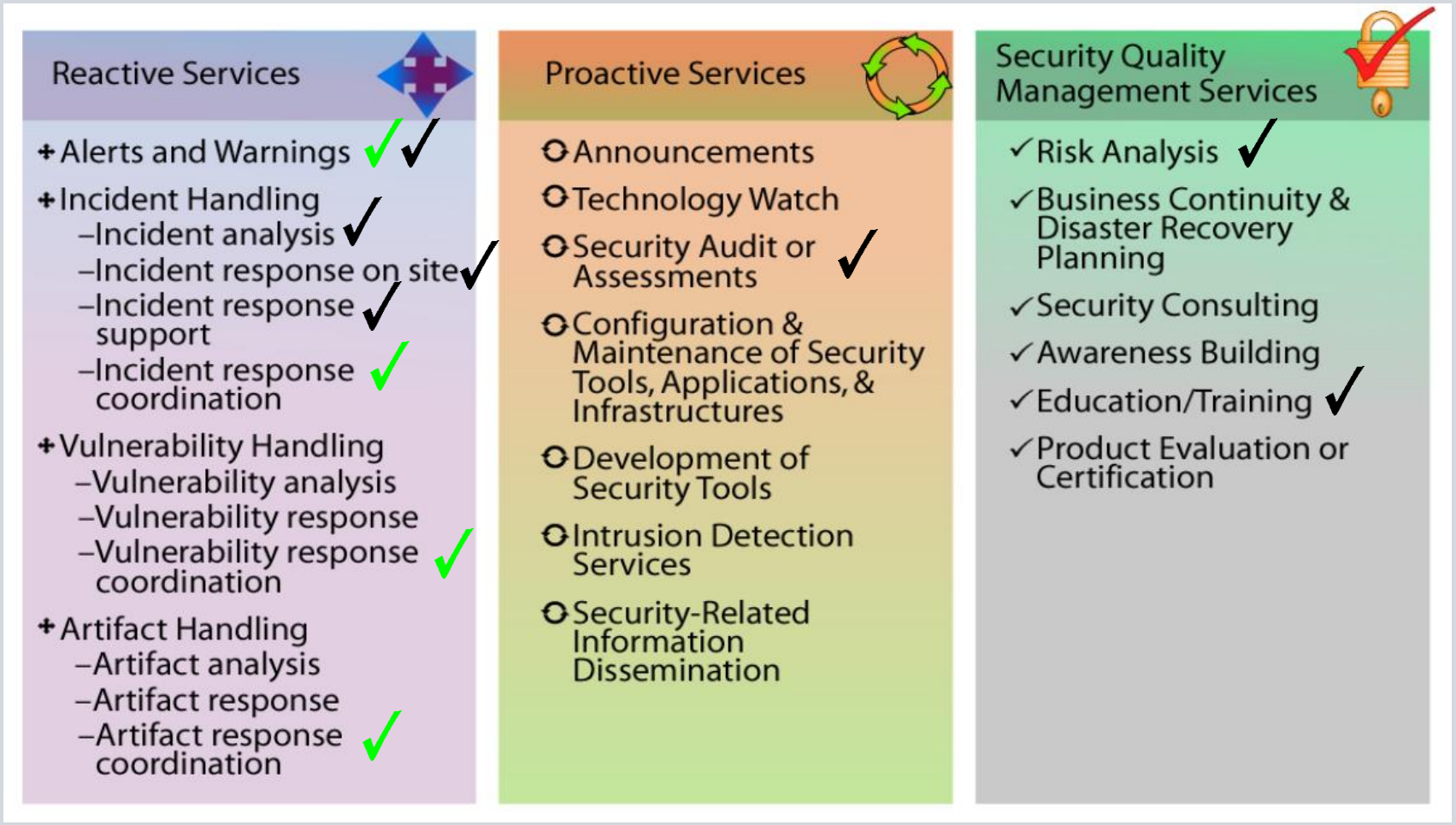
  Kompetensi Staff yang dibutuhkan dapat berupa standar kompetensi **Personal Skills**.

- **CSIRT memiliki Tim Internal Penanganan Insiden**

  Kompetensi Staff yang dibutuhkan berupa standar kompetensi pada kategori **Personal Skills, Technical Foundation and Incident Handling Skills**

BADAN SIBER & SANDI NEGARA

LAYANAN CSIRT



Standar Layanan Model CSIRT Koordinasi (✓)

Standar Layanan Model CSIRT memiliki Tim Internal Penanganan Insiden (✓)

Standar Layanan tersebut merupakan syarat minimal Layanan yang harus dimiliki oleh CSIRT

BADAN SIBER & SANDI NEGARA

PELAPORAN INSIDEN KEAMANAN SIBER

Insiden Keamanan Siber

Laporkan anomali

Deteksi dan Analisis oleh Pemilik Sistem

Dilaporkan beserta buktinya

CSIRT
Computer Security Incident Response Team

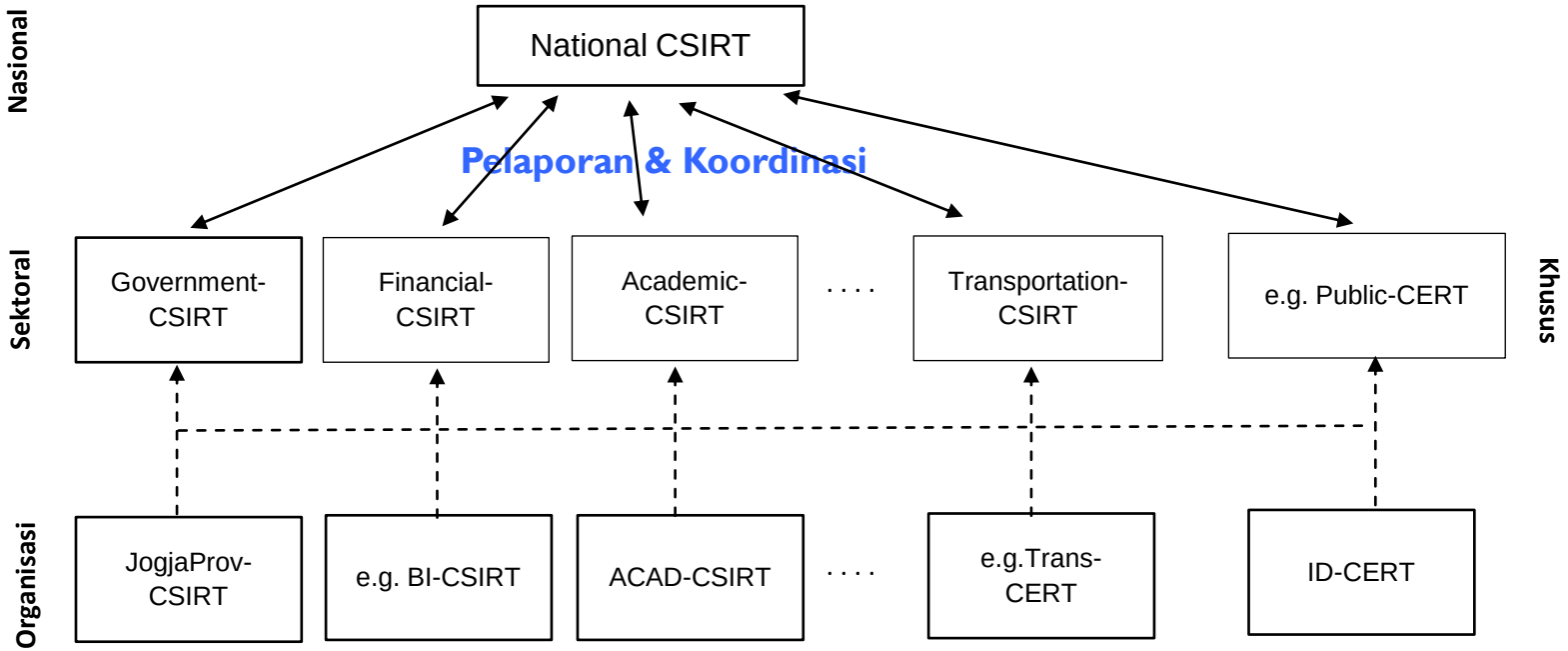
Penanganan Insiden Keamanan Siber dilakukan oleh CSIRT Internal

BADAN SIBER & SANDI NEGARA

JIKA INSIDEN TIDAK DAPAT TERTANGANI

BADAN SIBER &
SANDI NEGARA

KOORDINASI *CSIRT* DALAM LINGKUP NASIONAL



National CSIRT
(Tim Penanggulangan dan Pemulihan Insiden Siber Nasional)

- National CSIRT untuk mengelola Penanggulangan dan Pemulihan Insiden Siber secara nasional
- National CSIRT dibentuk dan diselenggarakan oleh BSSN
- National CSIRT menerima pendaftaran CSIRT

Sumber : Rancangan Peraturan BSSN tentang Tim Penanggulangan dan Pemulihan Insiden Siber.

BENEFIT MEMILIKI TIM CSIRT DAN TEREGISTRASI PADA GOV-CSIRT BSSN

1. **Tidak ada biaya keanggotaan** Gov-CSIRT
2. Menjadi prioritas sebagai peserta dalam kegiatan *Cyber Security Drill Test, Training* dan *Workshop* Keamanan Siber yang diselenggarakan oleh BSSN.
3. Memperoleh informasi terkait laporan tahunan insiden keamanan siber di Indonesia.

BADAN SIBER & SANDI NEGARA

BADAN SIBER &
SANDI NEGARA

TERIMA KASIH