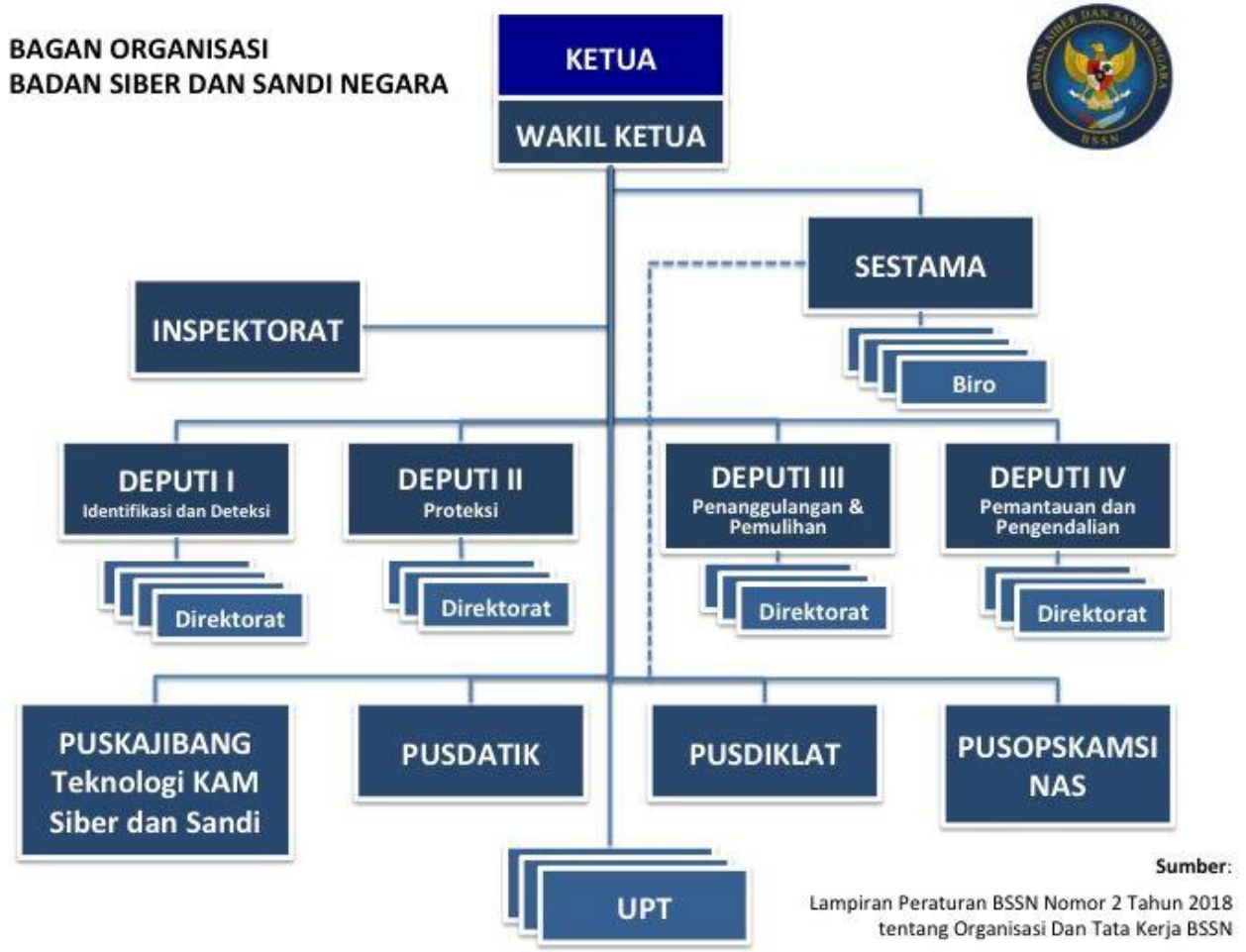
BADAN SIBER & SANDI NEGARA

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

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

SOTK BADAN SIBER SANDI NEGARA



BADAN SIBER & SANDI NEGARA

PENGGUNA INTERNET DI INDONESIA

Top 25 Countries, Ranked by Internet Users, 2013-2018
millions

	2013	2014	2015	2016	2017	2018
1. China*	620.7	643.6	669.8	700.1	736.2	777.0
2. US**	246.0	252.9	259.3	264.9	269.7	274.1
3. India	167.2	215.6	252.3	283.8	313.8	346.3
4. Brazil	99.2	107.7	113.7	119.8	123.3	125.9
5. Japan	100.0	102.1	103.6	104.5	105.0	105.4
6. Indonesia	72.8	83.7	93.4	102.8	112.6	123.0
7. Russia	77.5	82.9	87.3	91.4	94.3	96.6
8. Germany	59.5	61.6	62.2	62.5	62.7	62.7
9. Mexico	53.1	59.4	65.1	70.7	75.7	80.4
10. Nigeria	51.8	57.7	63.2	69.1	76.2	84.3
11. UK**	48.8	50.1	51.3	52.4	53.4	54.3
12. France	48.8	49.7	50.5	51.2	51.9	52.5
13. Philippines	42.3	48.0	53.7	59.1	64.5	69.3
14. Turkey	36.6	41.0	44.7	47.7	50.7	53.5
15. Vietnam	36.6	40.5	44.4	48.2	52.1	55.8
16. South Korea	40.1	40.4	40.6	40.7	40.9	41.0
17. Egypt	34.1	36.0	38.3	40.9	43.9	47.4
18. Italy	34.5	35.8	36.2	37.2	37.5	37.7
19. Spain	30.5	31.6	32.3	33.0	33.5	33.9
20. Canada	27.7	28.3	28.8	29.4	29.9	30.4
21. Argentina	25.0	27.1	29.0	29.8	30.5	31.1
22. Colombia	24.2	26.5	28.6	29.4	30.5	31.3
23. Thailand	22.7	24.3	26.0	27.6	29.1	30.6
24. Poland	22.6	22.9	23.3	23.7	24.0	24.3
25. South Africa	20.1	22.7	25.0	27.2	29.2	30.9
Worldwide* **	**2,692.9**	**2,892.7**	**3,072.6**	**3,246.3**	**3,419.9**	**3,600.2**

*Note: individuals of any age who use the internet from any location via any device at least once per month; *excludes Hong Kong; **forecast from Aug 2014; ***includes countries not listed*
Source: eMarketer, Nov 2014
181948 www.eMarketer.com

Mobile Phone Users
308,2 million (121% of population)

Smart Phone Users
63,4 million (24,7 % of population)

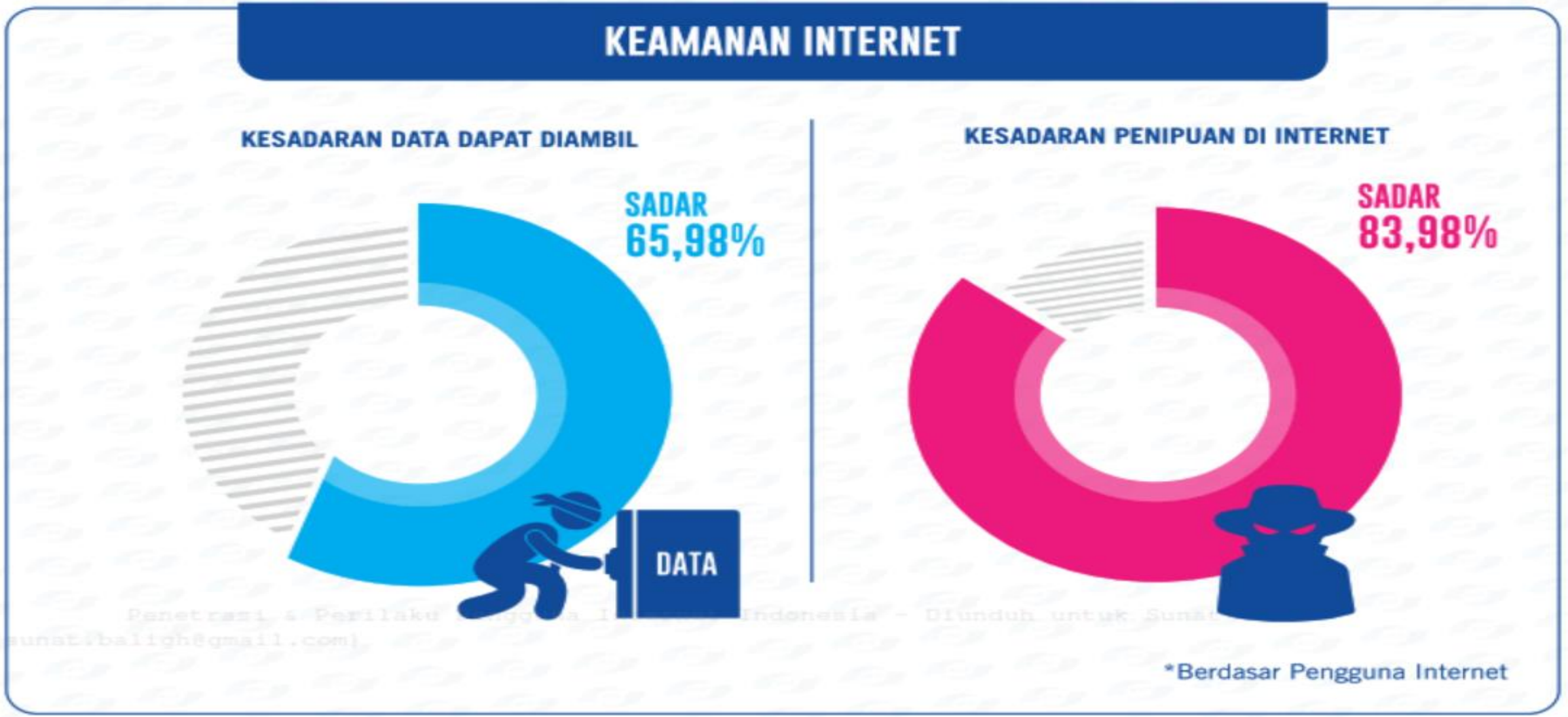
Age Composition
125 million people under the age of 35,
potential targets of e-commerce

Ranking Pengguna Internet Indonesia menduduki peringkat **7 Dunia**

Sumber : Hasil Survey Asosiasi Penyelenggara Internet Indonesia (APJII) 2017

BADAN SIBER & SANDI NEGARA

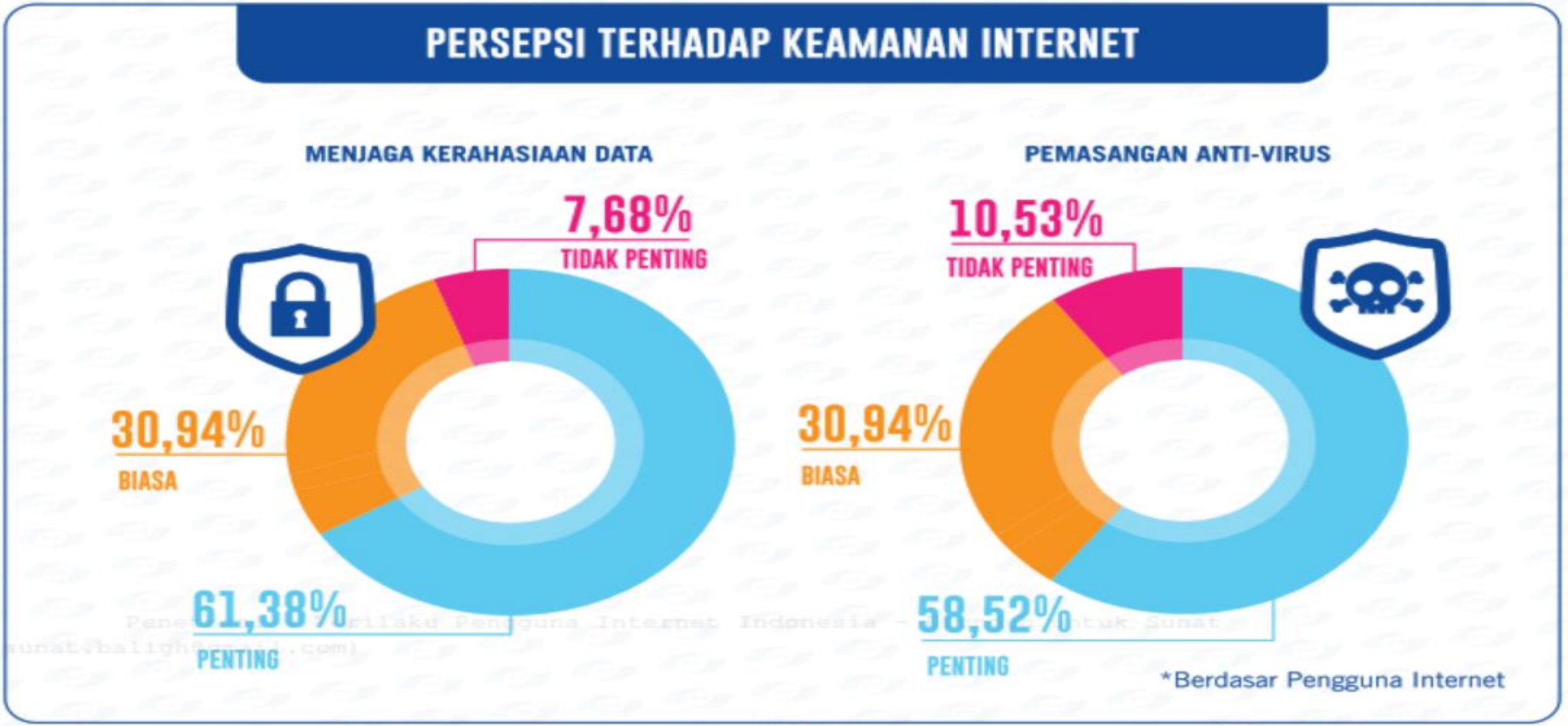
KEAMANAN INTERNET



Sumber : Hasil Survey Asosiasi Penyelenggara Internet Indonesia (APJII) 2017

BADAN SIBER & SANDI NEGARA

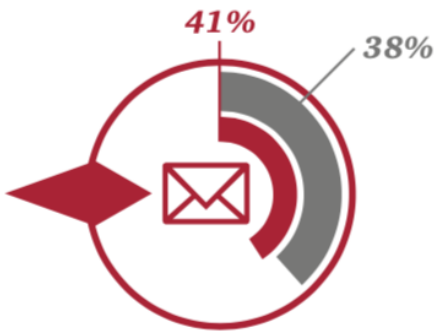
PERSEPSI TERHADAP KEAMANAN INTERNET



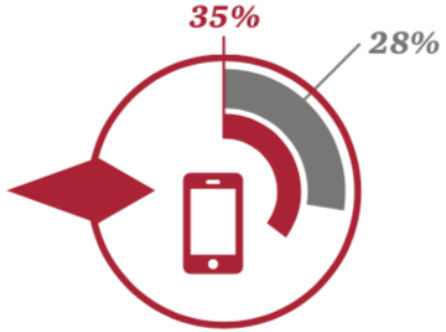
Sumber : Hasil Survey Asosiasi Penyelenggara Internet Indonesia (APJII) 2017

BADAN SIBER & SANDI NEGARA

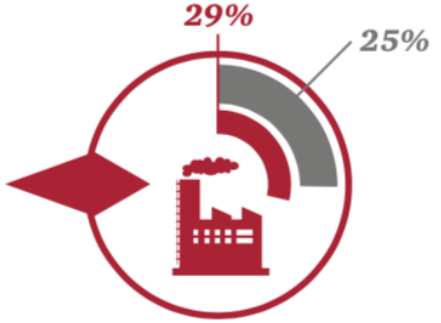
TOP VECTORS OF CYBER SECURITY INCIDENTS



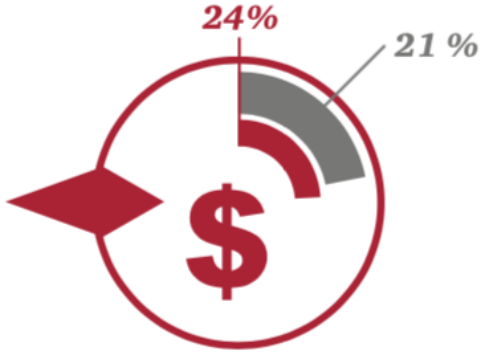
Phishing



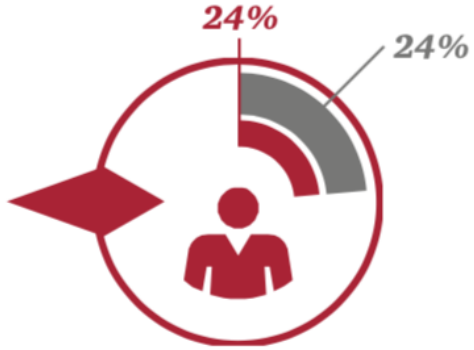
Mobile Device



Operational Technology



Financial Technology



Employee

Sumber: GSISS 2017

Sumber: Hasil Global State of Information Security Survey (GSISS) 2017

pwc

BADAN SIBER & SANDI NEGARA

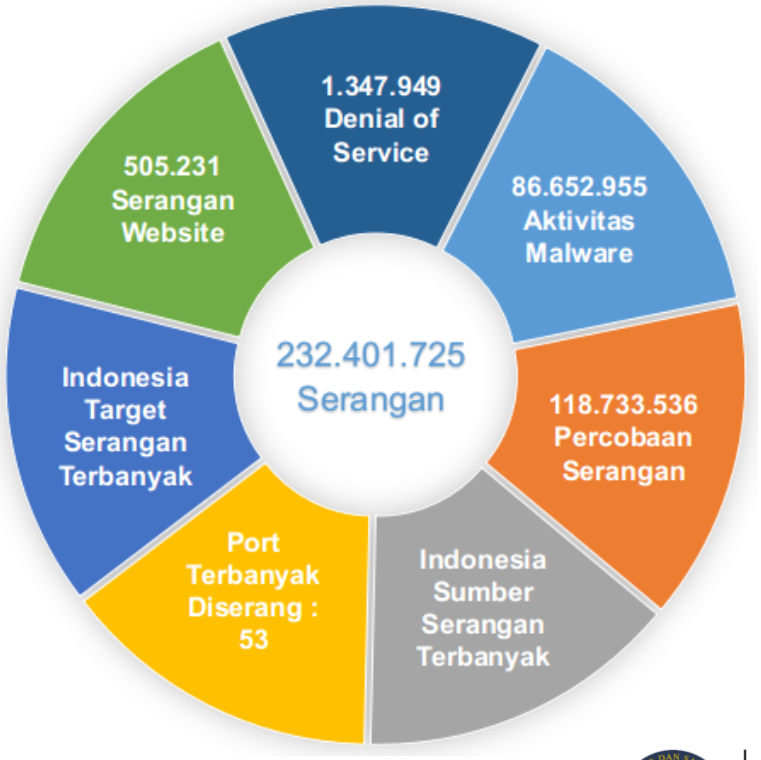
DATA SERANGAN SIBER DI INDONESIA

2017

Sumber : BSSN (ID-SIRTII)

11 %

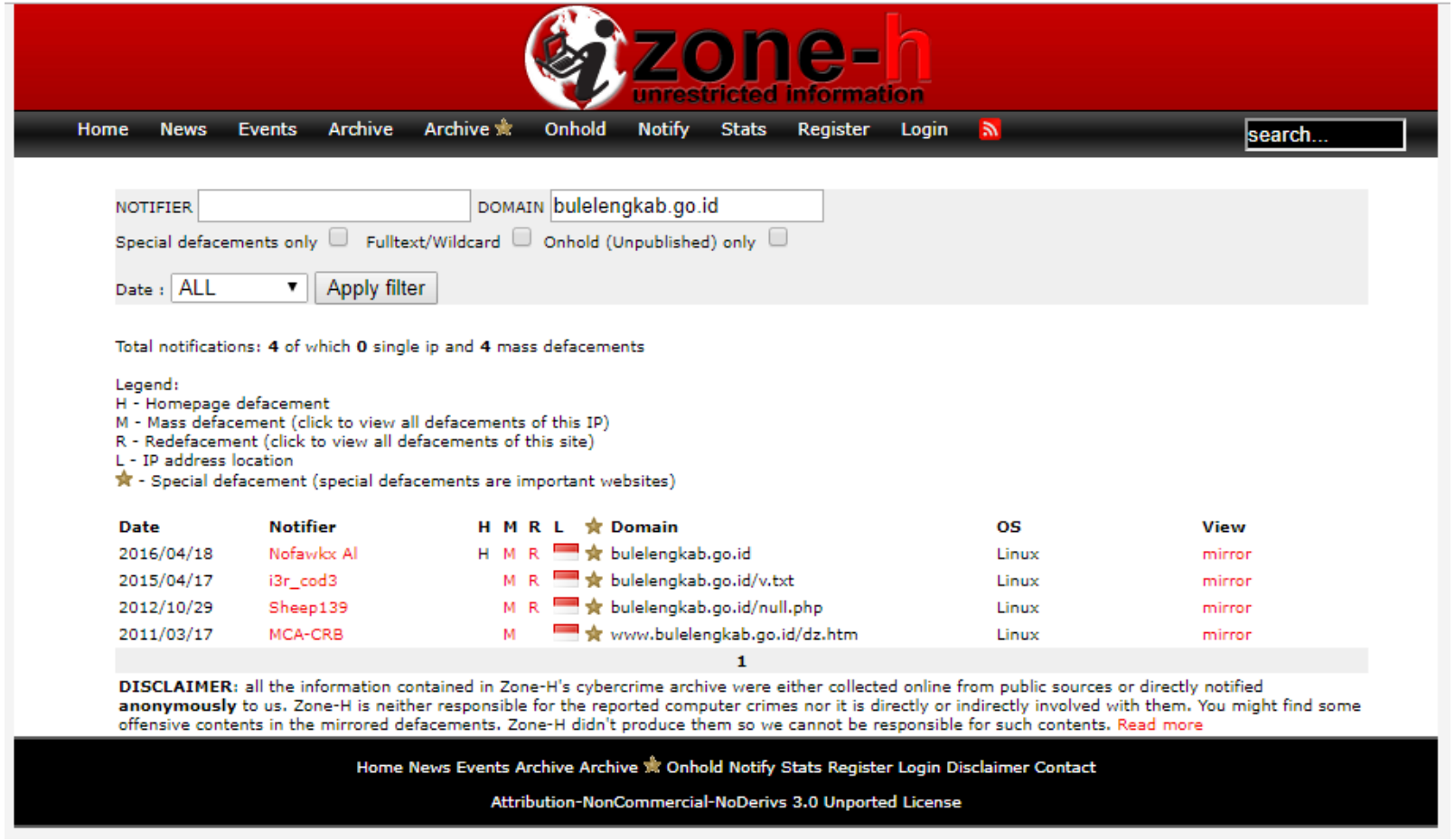
2018



Sumber : BSSN (ID-SIRTII)

BADAN SIBER & SANDI NEGARA

DATA SERANGAN SIBER PADA KAB. BULELENG BERDASARKAN ZONE - H



zone-h
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login search...

NOTIFIER DOMAIN bulelengkab.go.id

Special defacements only Fulltext/Wildcard Onhold (Unpublished) only

Date : ALL Apply filter

Total notifications: **4** of which **0** single ip and **4** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2016/04/18	Nofawkx Al	H	M	R		★	bulelengkab.go.id	Linux	mirror
2015/04/17	i3r_cod3		M	R		★	bulelengkab.go.id/v.txt	Linux	mirror
2012/10/29	Sheep139		M	R		★	bulelengkab.go.id/null.php	Linux	mirror
2011/03/17	MCA-CRB		M			★	www.bulelengkab.go.id/dz.htm	Linux	mirror

1

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. Read more

Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

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

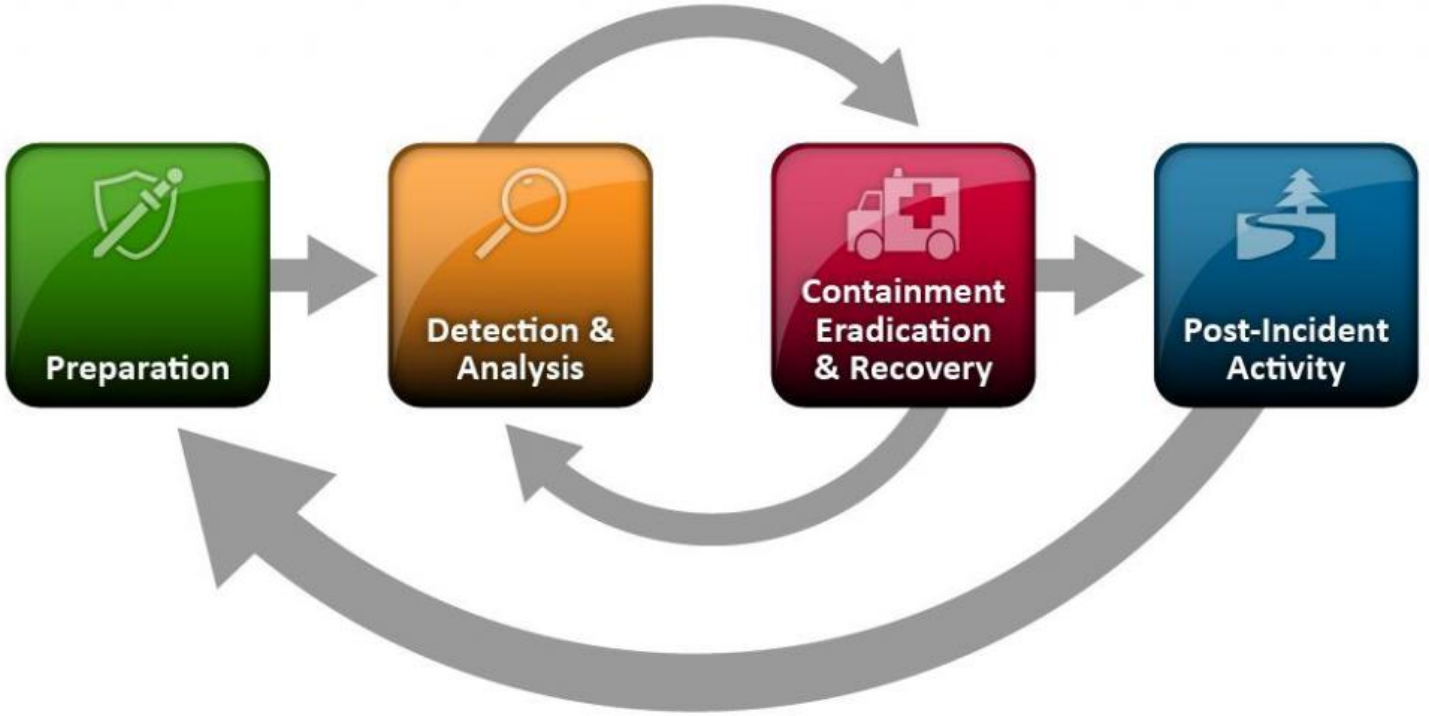
RESPON INSIDEN KEAMANAN SIBER

Penanganan Insiden Keamanan Siber merupakan sebuah usaha untuk mendeteksi, melaporkan, menilai, menangani dan merespon serta mempelajari insiden keamanan siber

Respon Insiden Keamanan Siber merupakan sebuah usaha yang dilakukan untuk memitigasi, memperbaiki dan atau mengembalikan sebuah Sistem Elektronik ke kondisi normal.

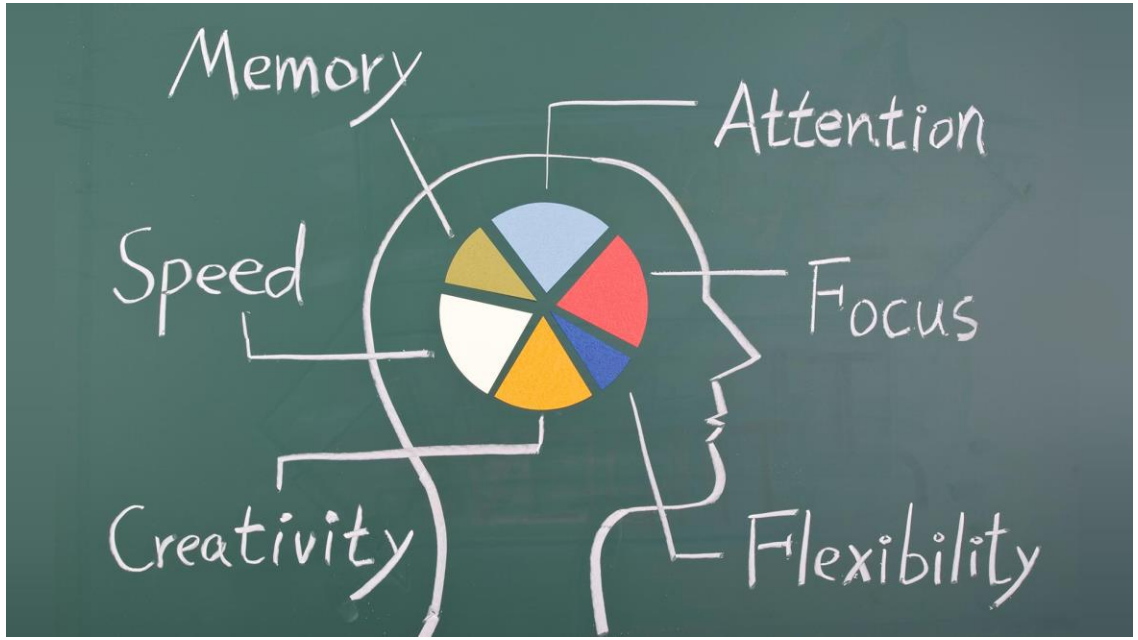
BADAN SIBER & SANDI NEGARA

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

PELAPORAN INSIDEN KEAMANAN SIBER

INSIDEN KEAMANAN SIBER

Dilaporkan beserta buktinya

VERIFIKASI oleh Point of Contact (POC)

Diteruskan

CSIRT
Computer Security Incident Response Team

Penanganan Insiden Keamanan Siber dilakukan oleh CSIRT Internal

BADAN SIBER & SANDI NEGARA

PELAPORAN insiden keamanan siber bssn

BADAN SIBER &
SANDI NEGARA

COMPUTER SECURITY INCIDENT RESPONSE TEAM (csirt)

- CSIRT : Organisasi atau tim yang bertanggung jawab untuk menerima, meninjau, dan menanggapi laporan dan aktivitas insiden keamanan siber.

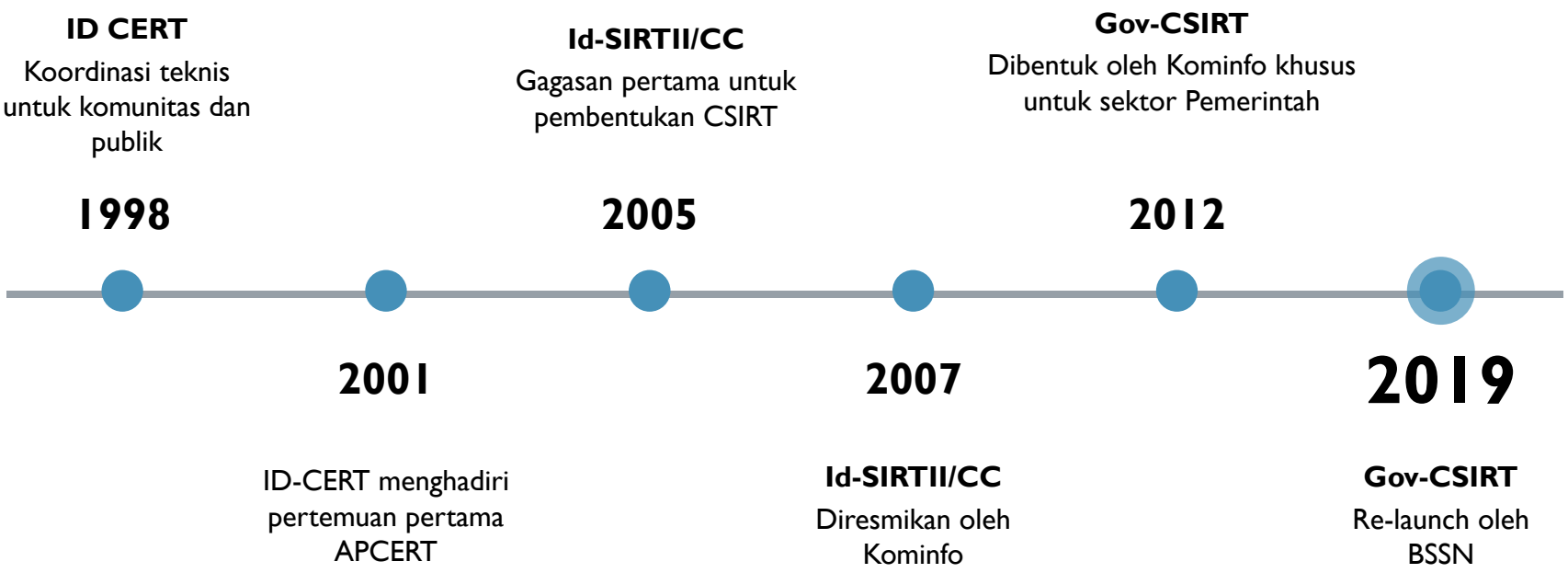
- Tujuan :
  - Melakukan **penyelidikan komprehensif** dan melindungi sistem atau data atas insiden keamanan siber yang terjadi pada organisasi.
  - Melakukan **pencegahan insiden** dengan cara terlibat aktif pada penilaian dan deteksi ancaman, perencanaan mitigasi, dan tinjauan atas arsitektur keamanan informasi organisasi.
- CSIRT harus **mampu beradaptasi** dengan lingkungan yang terus berkembang dan menghadirkan fleksibilitas untuk menangani setiap kejadian tak terduga.

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.

CERT/CSIRT DI INDONESIA



BADAN SIBER & SANDI NEGARA

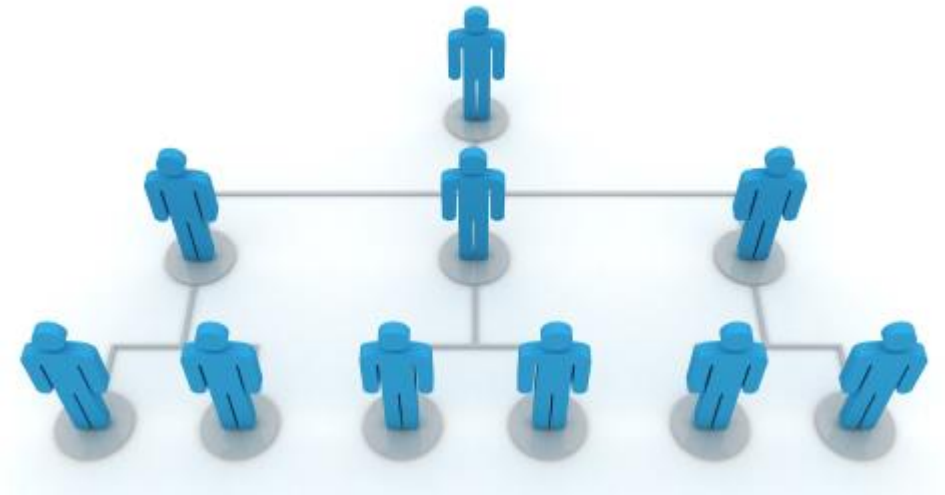
BAGAIMANA CSIRT BEKERJA?

CSIRT bekerja dengan menjalankan fungsi reaktif maupun kombinasi reaktif dan proaktif yang bertujuan untuk membantu melindungi dan mengamankan aset kritikal Organisasi dan Konstituen

BADAN SIBER & SANDI NEGARA

DIMANA CSIRT DITEMPATKAN ?

Tidak ada Standar tentang Lokasi CSIRT Organisasi harus berada di dalam sebuah divisi tertentu. Melainkan CSIRT merupakan bagian dari Penyelenggaraan **Keamanan Informasi** dan **Teknologi Informasi Komunikasi (TIK) sehingga CSIRT dilaksanakan oleh Organisasi Perangkat Daerah 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

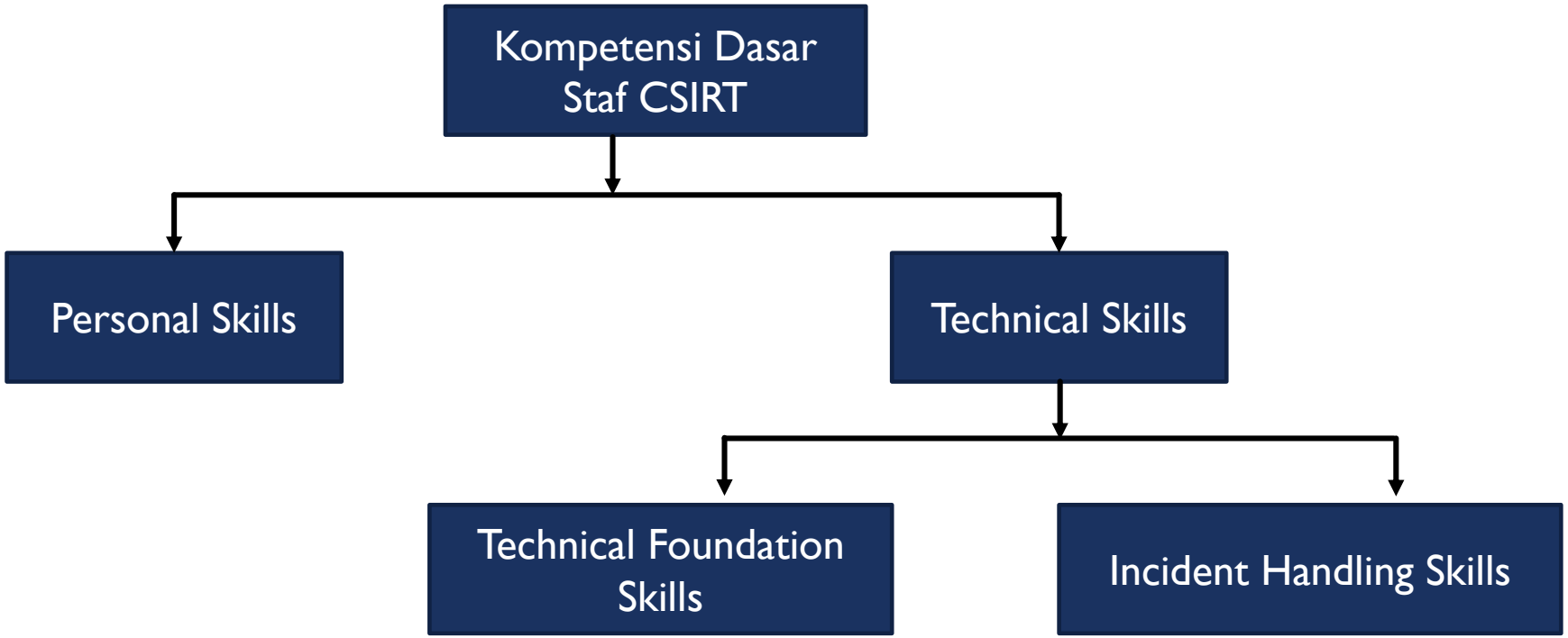
- Model CSIRT yang dipilih

  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



BADAN SIBER & SANDI NEGARA

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

BADAN SIBER & SANDI NEGARA

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

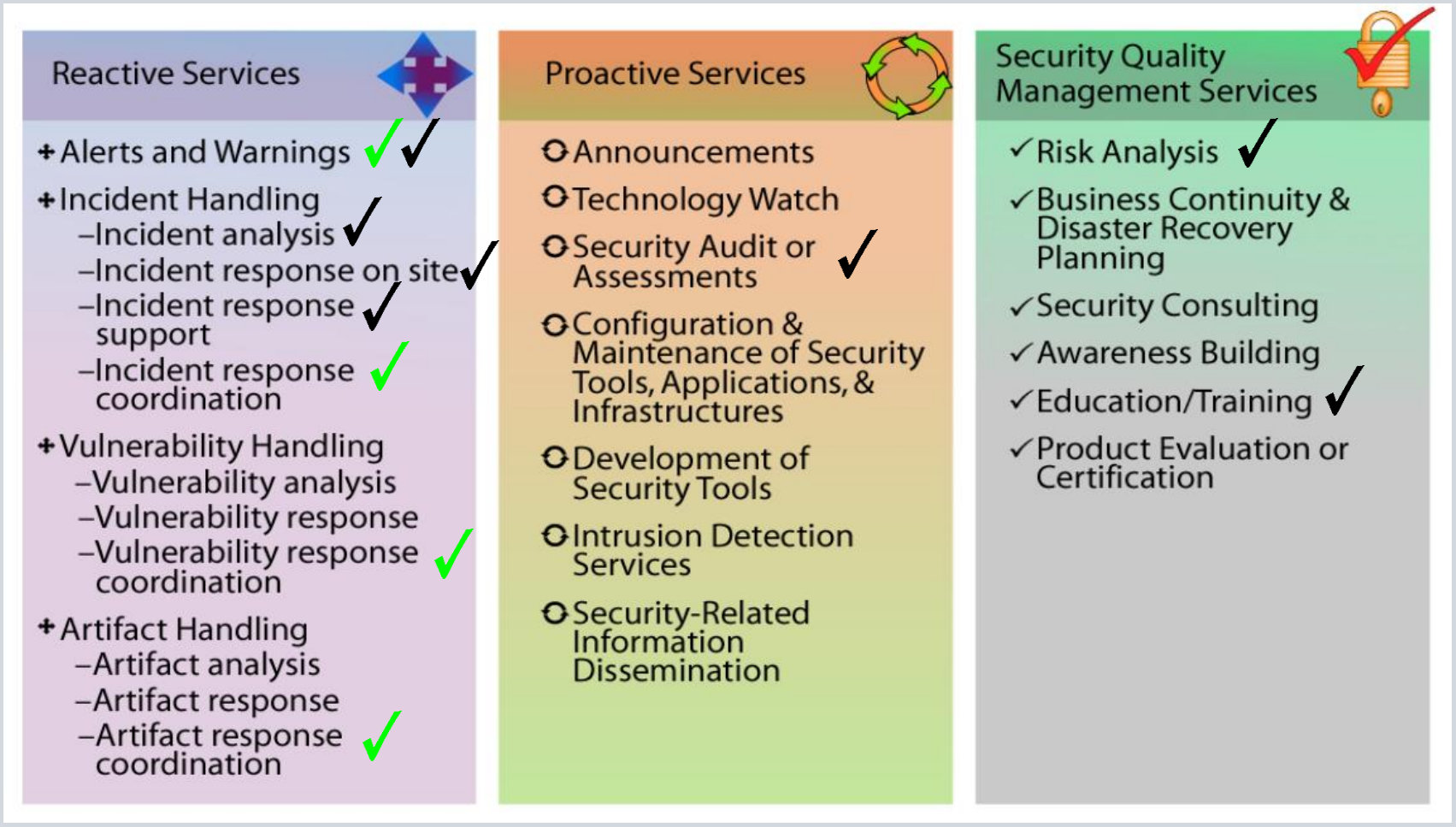
- **CSIRT Koordinasi**

  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**

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

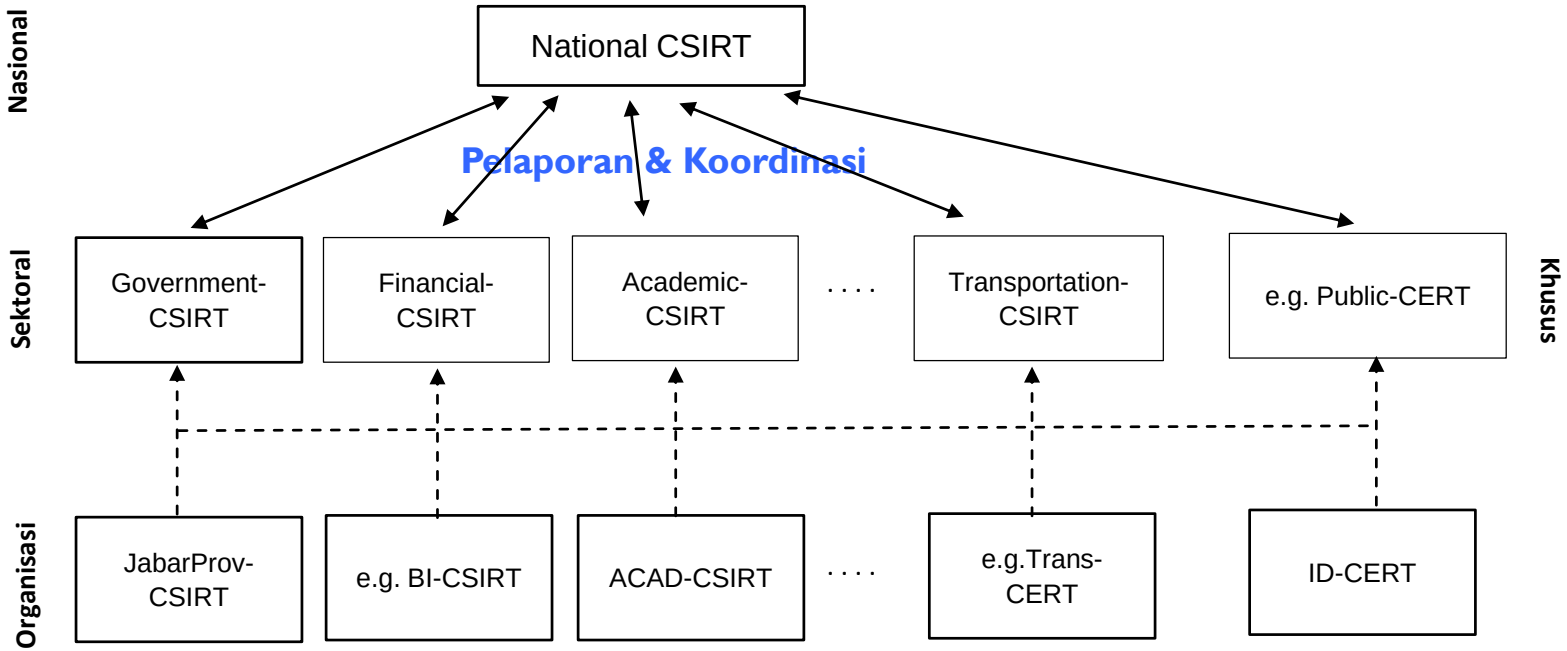
BADAN SIBER & SANDI NEGARA

BENEFIT MEMILIKI TIM CSIRT DAN TEREGISTRASI PADA GOV-CSIRT BSSN

1. **Tidak ada biaya keanggotaan** CSIRT Sektor Pemerintah
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

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.

BADAN SIBER & SANDI NEGARA

BADAN SIBER &
SANDI NEGARA

TERIMA KASIH