GOVERNMENT CSIRT

Direktorat penanggulangan dan Pemulihan Pemerintah
Badan Siber dan Sandi Negara

https://www.bssn.go.id
https://govcsirt.bssn.go.id

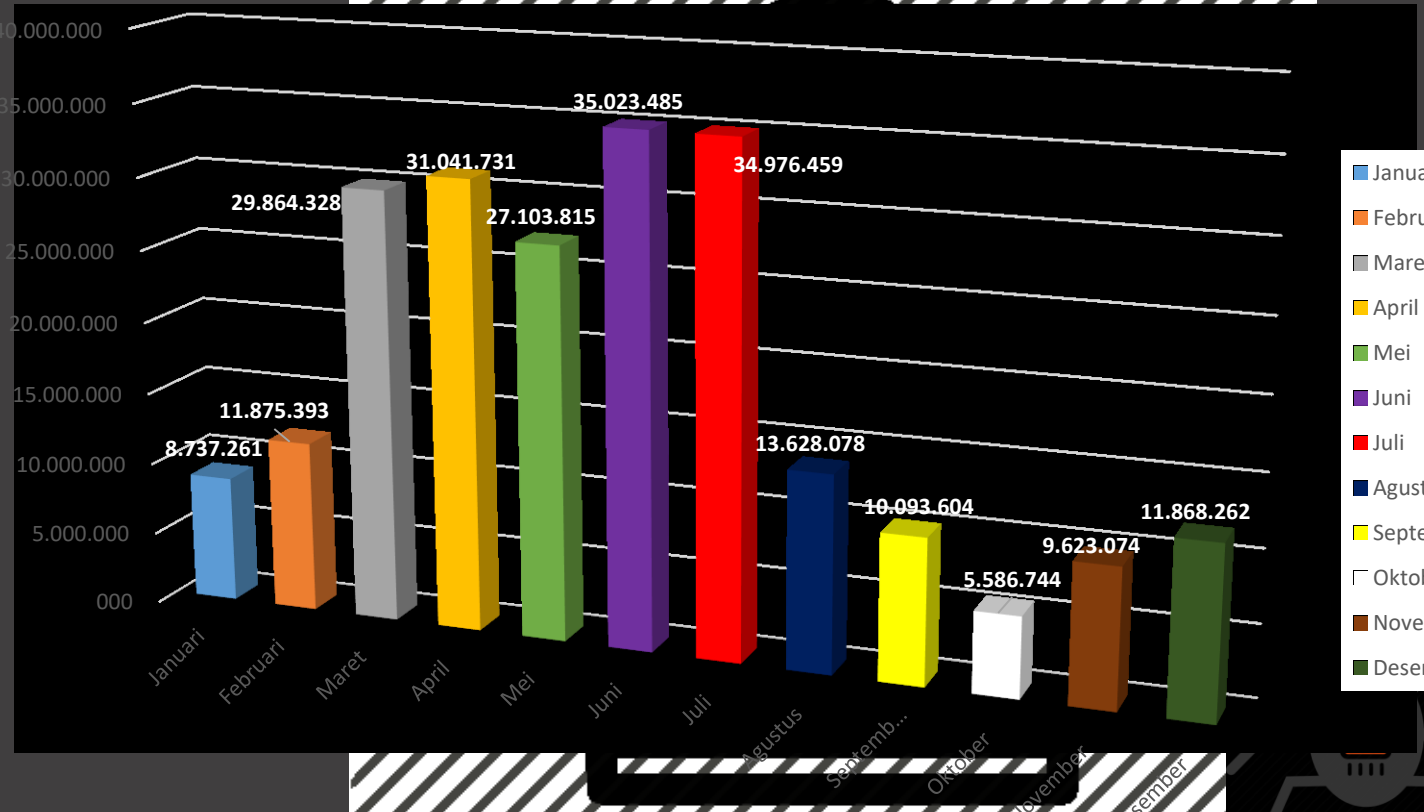
OUTLINE/PEMBAHASAN

- Visi BSSN
- Data Serangan Siber Tahun 2018
- Penjelasan CSIRT: Definisi, Sejarah, Manfaat, Layanan, Tipe, Macam/Jenis
- Gov-CSIRT Indonesia: Definisi, Misi, Konstituen dan Layanan, Panduan yang Telah Disediakan
- Tahapan Pembentukan CSIRT
- Layanan CSIRT, Pola Hubungan, Kebutuhan Pembentukan CSIRT

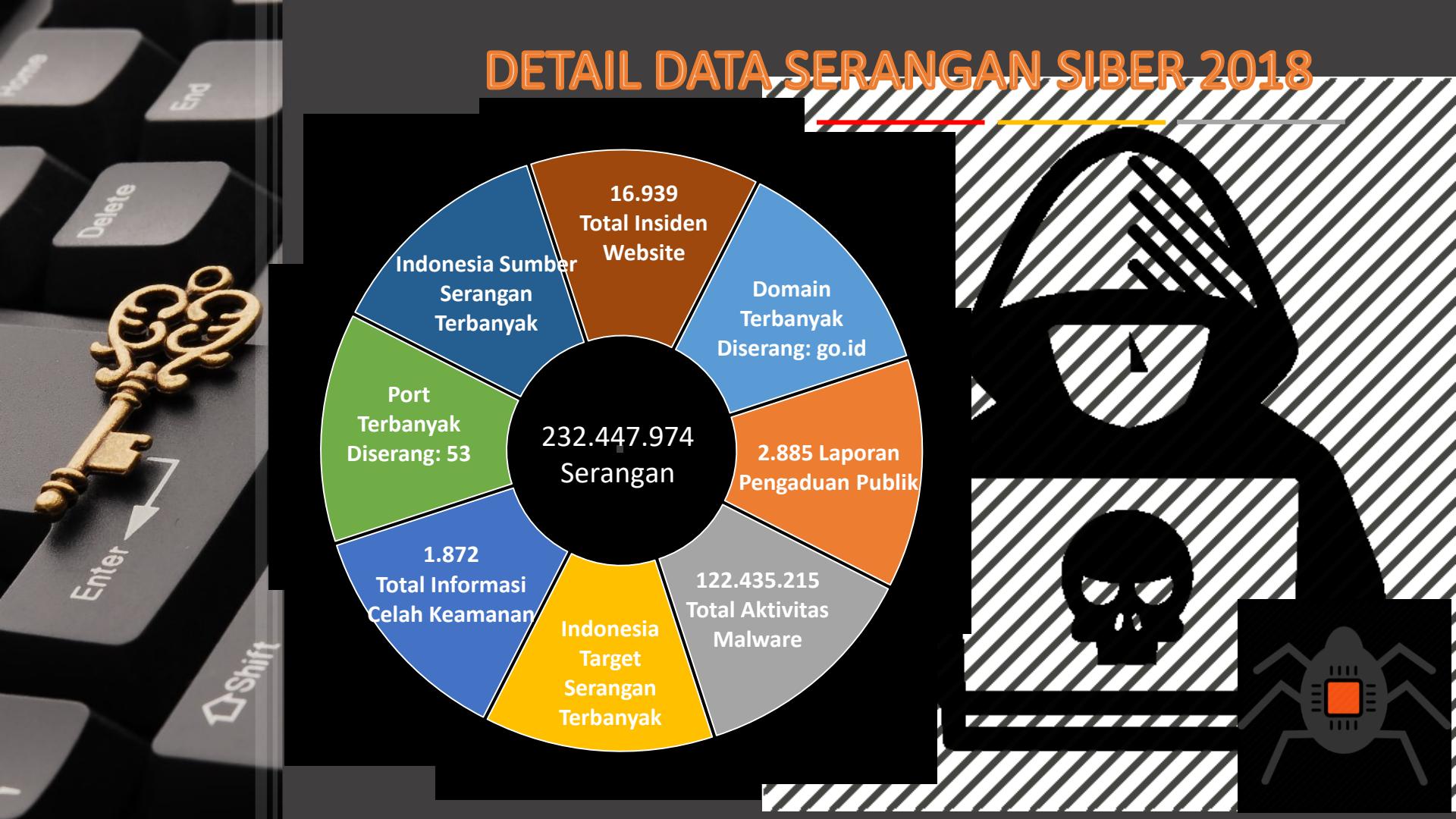
VISI BSSN

Menjadi institusi tepercaya dalam menjaga keamanan Siber dan Sandi Negara dengan menyinergikan berbagai pemangku kepentingan untuk ikut serta mewujudkan keamanan nasional dan meningkatkan pertumbuhan ekonomi nasional

DATA SERANGAN SIBER 2018 Per Bulan



DETAIL DATA SERANGAN SIBER 2018



Insiden

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 terhadap sistem atau informasi

PENYELENGGARAAN SISTEM ELEKTRONIK

PASAL 15 DAN 16 UU ITE

Kewajiban Penyelenggara Sistem Elektronik
1) Keandalan
2) Keamanan
3) Pertanggungjawaban

dapat melindungi keotentikan, integritas, kerahasiaan, ketersediaan, dan keteraksesan

tersedianya prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik yang didokumentasikan

menjamin penggunaan atau pengungkapan data dilakukan berdasarkan persetujuan dari pemilik Data Pribadi tersebut

BADAN SIBER
DAN SANDI NEGARA

CSIRT

Computer Security Incident Response Team

- CSIRT dianggap sebagai tim atau entitas dalam suatu lembaga yang menyediakan layanan dan dukungan kepada organisasi untuk mencegah, mengelola dan menanggapi insiden keamanan informasi.

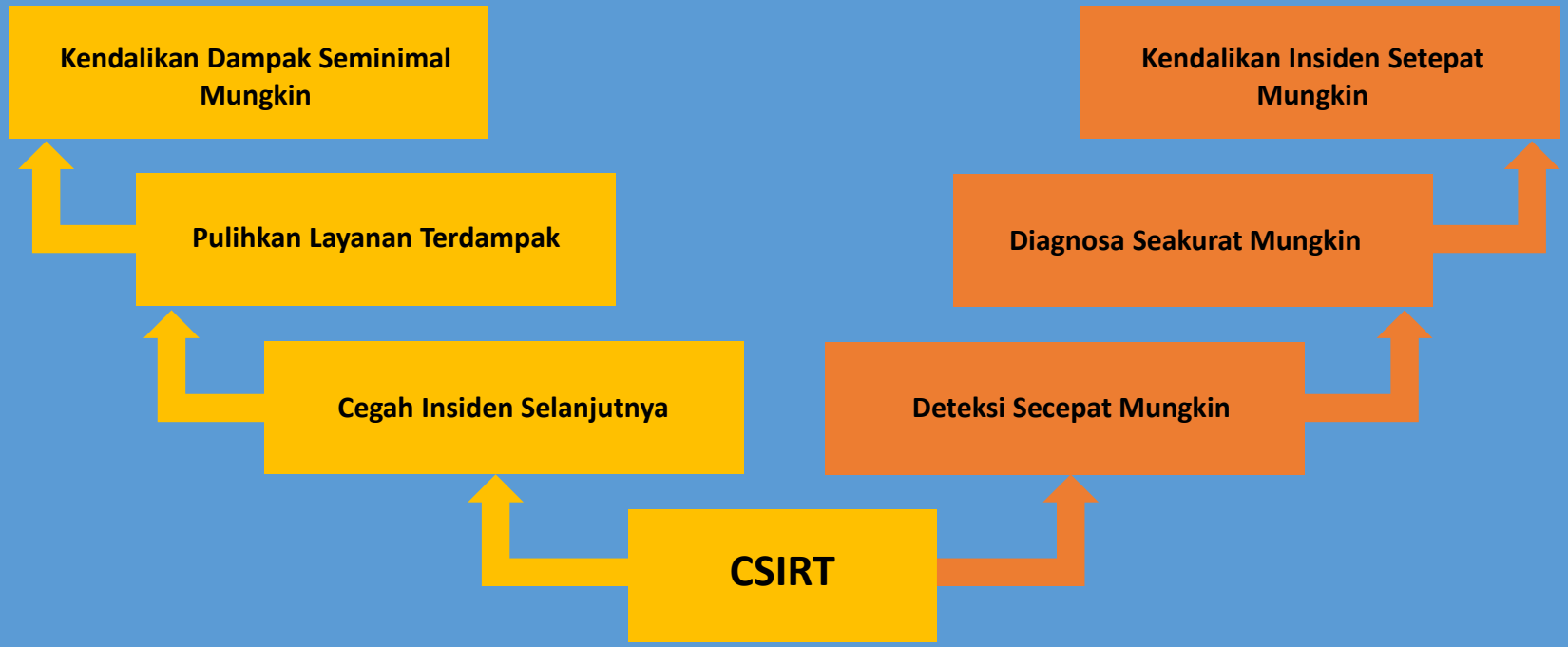
- Tim-tim ini biasanya terdiri dari para spesialis yang bertindak sesuai dengan prosedur dan kebijakan untuk merespon dengan cepat dan efektif terhadap insiden keamanan dan untuk mengurangi risiko serangan cyber.

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.

MANFAAT CSIRT



APA YANG CSIRT LAKUKAN

CSIRT Secara Umum

- ✓ Menyediakan *Point of Contact* (PoC) Tunggal untuk pelaporan
- ✓ Melakukan identifikasi dan Analisa terhadap apa yang terjadi termasuk dampak dan ancaman
- ✓ Strategi mitigasi dan solusi penelitian
- ✓ Berbagi informasi dan *lesson learned*

Tujuan CSIRT

- ❑ Meminimalisasi dan mengontrol kerusakan
- ❑ Memberikan asistensi respon dan pemulihan secara efektif
- ❑ Membantu pencegahan insiden terulang kembali

TIPE - TIPE CSIRT

Akademik CSIRT : Menyediakan layanan penanganan insiden kepada Akademik dan Institusi Pendidikan. Misalkan : ACAD-CSIRT (acad-csirt.com)

Internal CSIRT : Menyediakan layanan penanganan insiden kepada organisasi induk. Misalkan Bank, Perusahaan Manukfaktur, Universitas

Sektor Critical Information Protection (CIP) CSIRT : Menyediakan layanan penanganan insiden kepada penyedia layanan informasi/infrastruktur kritikal.

Sektor Pemerintah CSIRT : Menyediakan layanan penanganan insiden kepada stakeholder pemerintah. Misalkan : Gov-CSIRT, Jabar-CSIRT, Jogja-PGCSIRT, dll

National CSIRT : Sebagai kontak poin penyelenggaraan CSIRT di setiap negara

MACAM - MACAM ORGANISASI CSIRT

FIRST	FIRST - Forum of Incident Response and Security Teams (Global / International Initiatives)
APCERT	FIRST - Asian Pacific Computer Emergency Response Team (Regional Asia Pacific)
OIC-CERT	FIRST - Organization of Islamic Conference - Computer Emergency Response Team
ENISA	FIRST - European Network and Information Security Agency (Regional Europe Union)
TF-CSIRT	FIRST - Collaboration of Computer Security Incident Response Team in Europe

https://www.first.org

Search

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog

Sign in

Current FIRST SIGs

Academic Security SIG
Space for discussion in order to reflect on our collective experiences, focus on current challenges and envision strategies on how we could work together to improve security in academic environments.

Big Data SIG
Incident Detection and Response at Scale.

Capture the Flag SIG
Designs, develops, and conducts security challenge and competition exercises for the FIRST.org community.

CVSS SIG: Common Vulnerability Scoring System
For a global approach towards scoring metrics for vulnerabilities.

Cyber Threat Intelligence SIG
To define Threat Intelligence in the commercial space.

Ethics SIG
The Ethics SIG seeks to further the professionalization of the FIRST Community and improve the global understanding of SIRTs through the development of an ethical code for FIRST Members.

ICS SIG: Industrial Control Systems
In ICS-SIG we bring together expertise from several sectors to create processes.

Events at spotlight

FIRST is the global Forum of Incident Response and Security Teams

FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services. Some of these are:

- access to up-to-date best practice documents
- technical colloquia for security experts
- hands-on classes
- annual incident response conference
- publications and web services
- special interest groups

Currently FIRST has more than 400 members, spread over Africa, the Americas, Asia, Europe and Oceania.

What's New

Maturity Level 3 (Advanced) - Proactive...we're ready for anything (mostly)
Hopefully what we've outlined as suggested services and functions a PSIRT could offer at the various stages of their development will be helpful and inspires your team to raise their game.
(Thu, 24 Jan 2019 14:00 +0000)

Maturity Level 2 (Intermediate) - I am reactive, but I've trained for it!
Are you mature, are you immature - what are you? Maturity Level 2 is about adapting the ad-hoc PSIRT strategies into full blown policies and processes.
(Wed, 23 Jan 2019 14:00 +0000)

The Beginning - a very fine place to start!
To start you on your path to PSIRT goodness, you'll want to read and digest the PSIRT Maturity Document created by your friendly global FIRST PSIRT representatives. And what's a better place to start than at the beginning?
(Tue, 22 Jan 2019 14:00 +0000)

What is FIRST to you?

Gov-CSIRT Indonesia

Definisi

- Government – Computer Security Incident Response Team (CSIRT) Indonesia, disingkat Gov-CSIRT Indonesia merupakan CSIRT sektor Pemerintah Indonesia yang ditetapkan oleh Kepala Badan Siber dan Sandi Negara dalam Keputusan Kepala Badan Siber dan Sandi Negara Nomor 570 Tahun 2018 tanggal 20 Desember 2018.
- Bertanggungjawab sebagai ketua Gov-CSIRT Indonesia adalah Direktur Penanggulangan dan Pemulihan Pemerintah pada Deputi Bidang Penanggulangan dan Pemulihan BSSN.
- Anggota Tim dari Gov-CSIRT Indonesia adalah seluruh staf BSSN pada sektor pemerintah dan anggota CSIRT Instansi Pemerintah.

Misi

- membangun, mengoordinasikan, mengolaborasikan dan mengoperasionalkan sistem mitigasi, manajemen krisis, penanggulangan dan pemulihan terhadap insiden keamanan siber pada sektor pemerintah;
- membangun kerja sama dalam rangka penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah;
- membangun kapasitas sumber daya penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah;
- mendorong pembentukan CSIRT (Computer Security Incident Response Team) pada sektor pemerintah.

BADAN SIBER
DAN SANDI NEGARA

Konstituen dan Layanan

- Konstituen dari Gov-CSIRT Indonesia meliputi seluruh Pemerintah Daerah dan Pemerintah Pusat.
- Gov-CSIRT Indonesia memberikan layanan yang meliputi respon insiden dalam bentuk:
  - triase insiden;
  - koordinasi insiden; dan
  - resolusi insiden.
  - Disertai dengan aktivitas proaktif dalam bentuk:
    - cyber security drill test;
    - workshop atau bimbingan teknis; dan
    - asistensi pembentukan CSIRT sektor pemerintah.

Panduan yang Telah Disediakan

- Panduan Pelaporan Insiden
- Panduan Penanganan Insiden Web Defacement
- Panduan Penanganan Insiden Serangan DDoS
- Panduan Penanganan Insiden Serangan Phishing
- Panduan Penanganan Insiden Serangan SQL Injection
- Panduan Penanganan Insiden Malware

BADAN SIBER
DAN SANDI NEGARA

Tampilan Website Gov-CSIRT Indonesia

Berita Gov-CSIRT Indonesia

BADAN SIBER
DAN SANDI NEGARA

PEMBENTUKAN CSIRT

TAHAPAN PEMBENTUKAN CSIRT

Tahap 1 Edukasi Organisasi

Organisasi ingin membangun CSIRT namun belum memahami tentang CSIRT.

Tahap 2 Perencanaan

Organisasi memahami CSIRT dan mulai melakukan identifikasi dan analisis berbagai macam isu yang terkait penerapan CSIRT

Tahap 3 Penerapan

CSIRT dibentuk dan mulai menyelenggarakan layanan.

Tahap 4 Fase Operasional

CSIRT melakukan penanganan insiden

Tahap 5 Evaluasi

CSIRT menjadi Tim yang matang, mempunyai pengalaman melakukan penanganan insiden dan berkolaborasi dengan CSIRT lain

Source : Carnegie Mellon University

LAYANAN CSIRT

Reactive Services

- Alerts and Warnings
- Incident Handling
  - –Incident analysis
  - –Incident response on site
  - –Incident response support
  - –Incident response coordination
- Vulnerability Handling
  - –Vulnerability analysis
  - –Vulnerability response
  - –Vulnerability response coordination
- Artifact Handling
  - –Artifact analysis
  - –Artifact response
  - –Artifact response coordination

Proactive Services

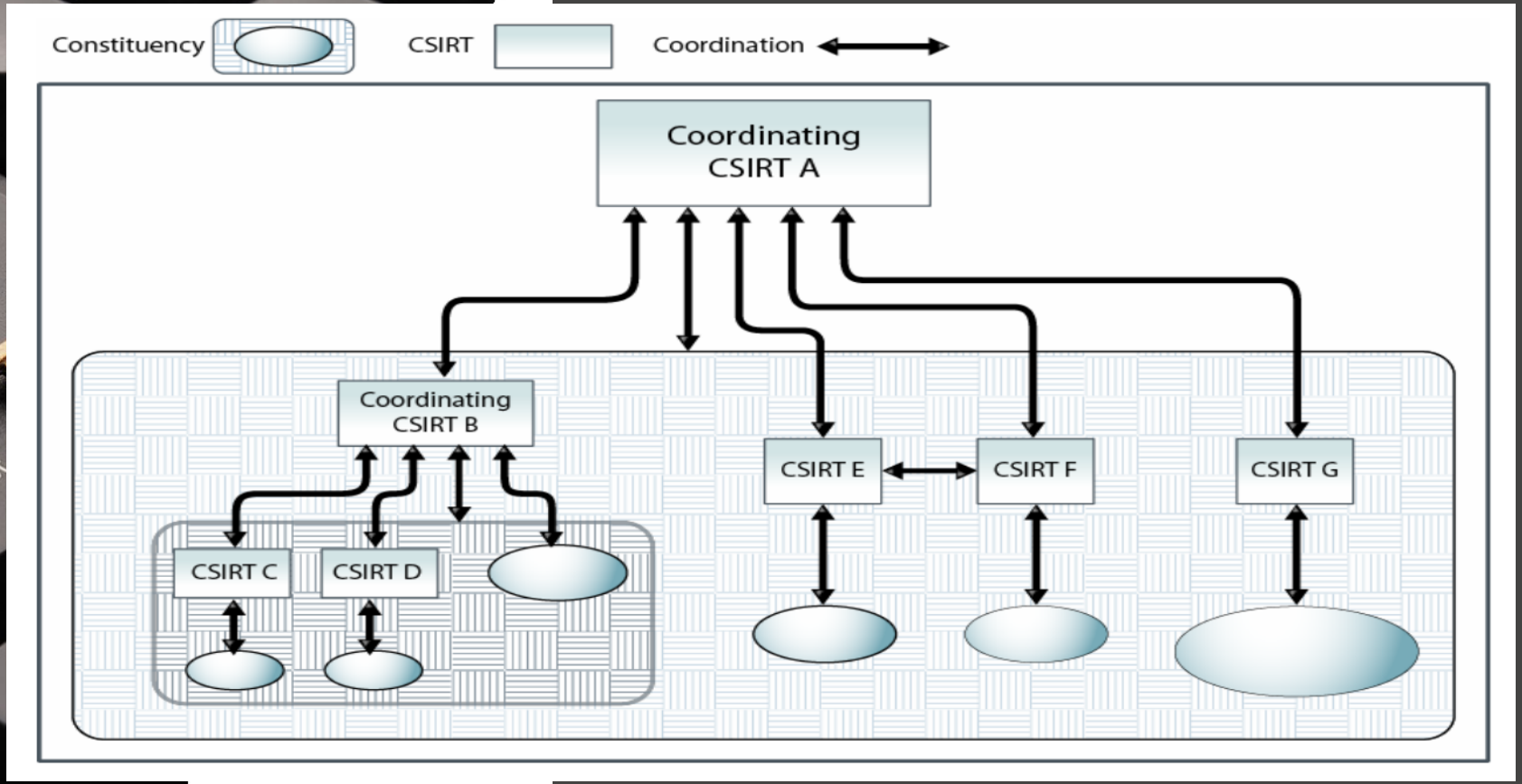
- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

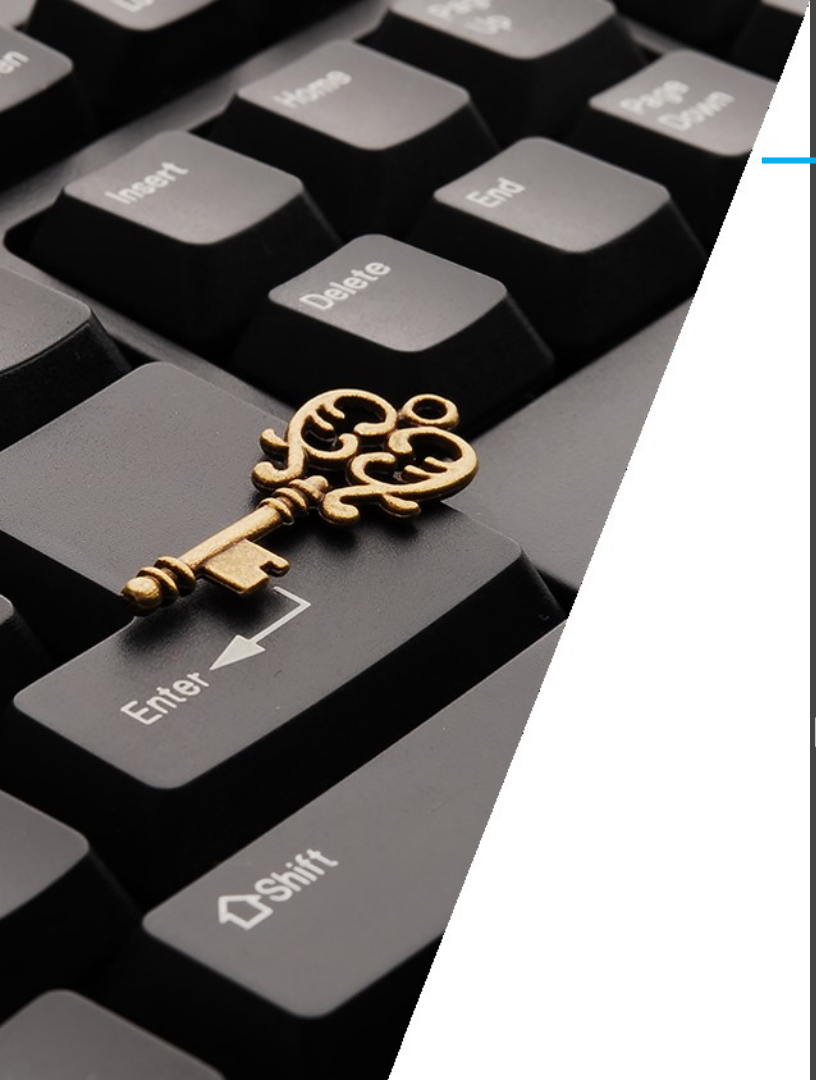
Security Quality Management Services

- ✓Risk Analysis
- ✓Business Continuity & Disaster Recovery Planning
- ✓Security Consulting
- ✓Awareness Building
- ✓Education/Training
- ✓Product Evaluation or Certification

Source: CERT. “Incident Management - CSIRT Services. Carnegie Mellon Univ Software Enginering Inst”

POLA HUBUNGAN CSIRT





KEBUTUHAN CSIRT

- Pembangunan Infrastruktur CSIRT
- Konsultasi Pengenalan CSIRT
- Partisipasi FGD Sektor Pemerintah
- Partisipasi Cyber Security Drill Test
- Sosialisasi CSIRT Kepada Konstituen
- Partisipasi Workshop Kemanan Informasi dan Siber
- Studi Banding CSIRT Dalam Negeri
- Partisipasi Seminar Keamanan Informasi dan Siber

BADAN SIBER
DAN SANDI NEGARA

TERIMA KASIH