GOV-CSIRT INDONESIA

REFRESHMENT
PENGELOLAAN CSIRT

Communication Check Bulan April Gov-CSIRT

Frizka Ferina

Jakarta, 21 April 2022

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

Sebuah organisasi atau kemampuan untuk menyediakan layanan serta dukungan kepada konstituen tertentu untuk mencegah, menangani, dan menanggapi insiden keamanan komputer.

PENAMAAN TIM TANGGAP INSIDEN

AKRONIM	DESKRIPSI
CERT	Computer Emergency Response Team
CSIRC	Computer Security Incident Response Capability or Center
CIRC	Computer Incident Response Capability or Center
CIRT	Computer Incident Response Team
IHT	Incident Handling Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

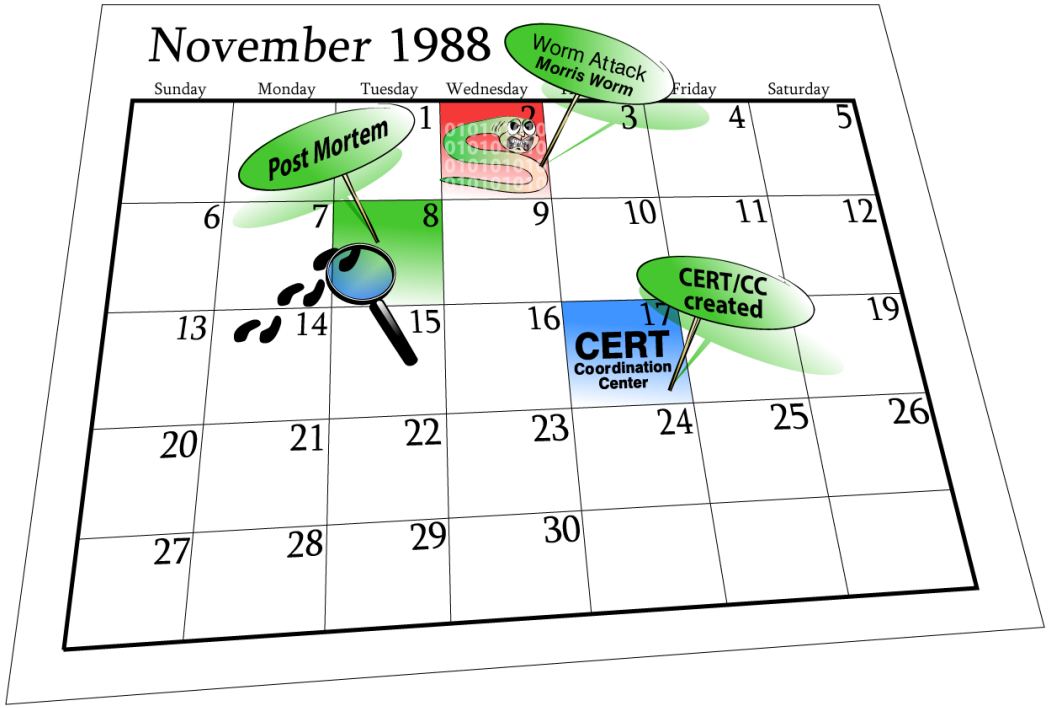
SEJARAH CSIRT

- Robert Tappan Morris (mahasiswa di Cornell University) pada 2 November 1988 mereplikasi worm komputer melalui Internet.
- Melumpuhkan hampir 10% (6000) komputer yang terhubung ke Internet pada November 1988.
- Dijatuhi hukuman percobaan tiga tahun, 400 jam pelayanan masyarakat, denda $10.050 ditambah biaya pengawasannya.

Morris ditemani oleh ibunya, Anne, kiri, dan ayahnya, Robert Sr., di belakang kanan, setelah persidangannya atas tuduhan menyusup ke jaringan komputer nasional pada November 1988

SEJARAH CSIRT

- Pada tanggal 7 November 1988, penyelesaian insiden tersebut dilakukan melalui kerjasama internasional.
- Ditandai dengan duplikasi usaha dan pemborosan sumber daya.
- Untuk menghadapi serangan serupa di masa yang akan datang, menghindari duplikasi upaya, pemborosan sumber daya, dan penyelesaian bersama, CERT pertama kali dibentuk.

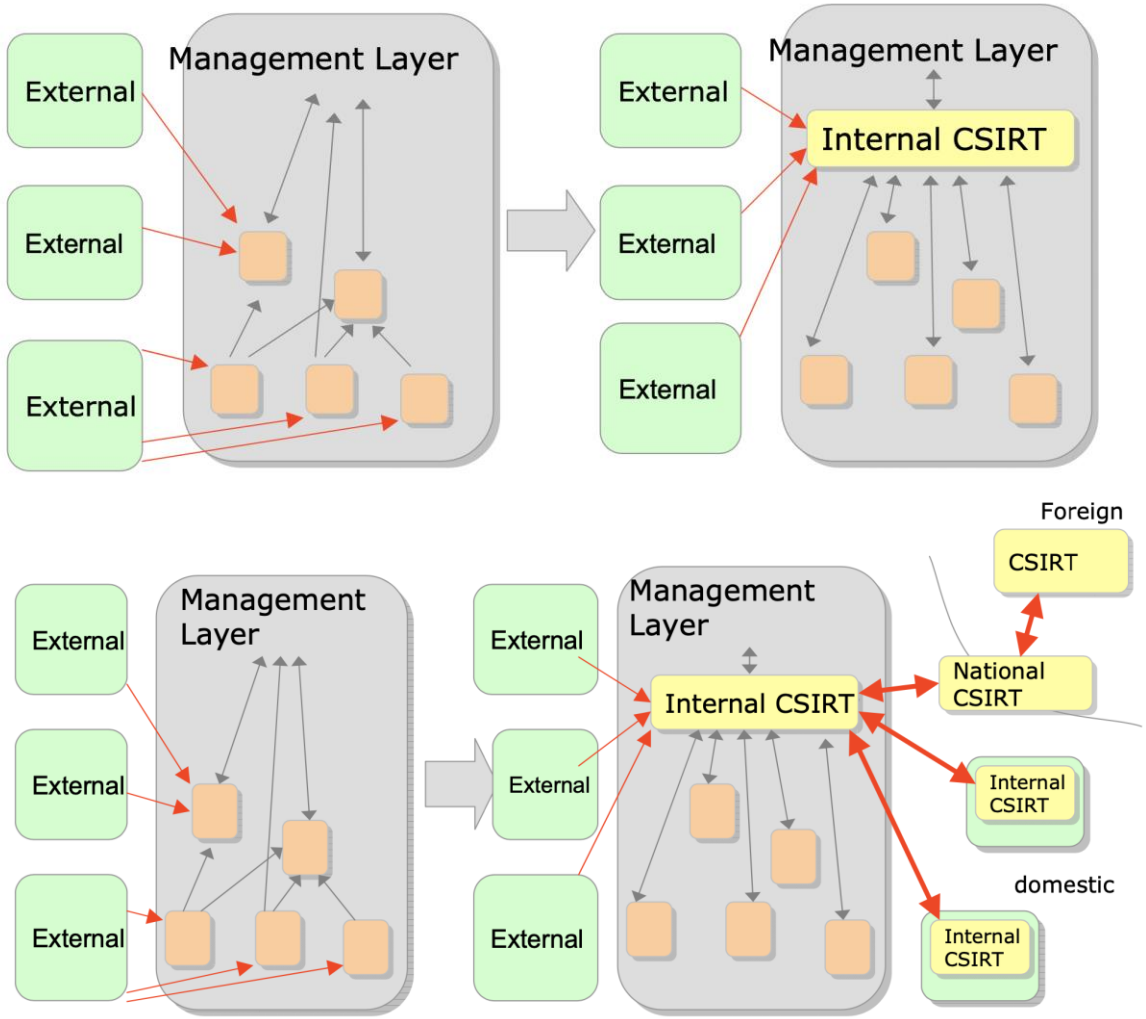


URGENSI CSIRT

- Mengelola informasi yang relevan dengan insiden.
  - ✓ Berbagi informasi keamanan serta manajemen informasi keamanan yang terpusat.
  - ✓ Penyederhanaan pengambilan keputusan untuk respon insiden.

- Menyediakan pusat *poin of contact*.
  - ✓ Pihak ketiga tepercaya yang mengkomunikasikan informasi insiden secara langsung.
  - ✓ Realisasi konsolidasi informasi dari luar.

- Membangun hubungan tepercaya yang diperlukan untuk merespon.
  - ✓ Meningkatkan konten informasi yang dibutuhkan untuk respon insiden.
  - ✓ Siap untuk merespon insiden.



APA YANG DILAKUKAN CSIRT

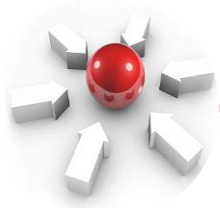
UMUM

- Menyediakan satu titik kontak untuk melaporkan masalah/insiden siber yang terjadi di lokal;
- Mengidentifikasi dan menganalisis apa yang telah terjadi termasuk dampak dan ancamannya;
- Mencari solusi dan strategi mitigasi;
- Berbagi opsi respons, informasi, dan pelajaran yang dipetik;
- Membangun kesadaran dan kapasitas di dalam dan di luar organisasi.

Tujuan CSIRT:

- Meminimalkan dan mengendalikan kerusakan;
- Memberikan atau membantu dengan respons dan pemulihan yang efektif;
- Membantu mencegah kejadian di masa depan.

MODEL CSIRT



CSIRT Sentral

Menangani insiden di seluruh organisasi;
Efektif untuk organisasi kecil.

CSIRT Terdistribusi

Memiliki beberapa CSIRT;
Efektif untuk organisasi besar;
Sumber komputasi utama di lokasi yang jauh.

CSIRT Koordinasi

Tidak memiliki sumber daya penanganan insiden;
CSIRT yang berkoordinasi dengan CSIRT lain.

MODEL CSIRT

Kompetensi Dasar Staf CSIRT

Personal Skills

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

Technical Skills

Technical Foundation Skills

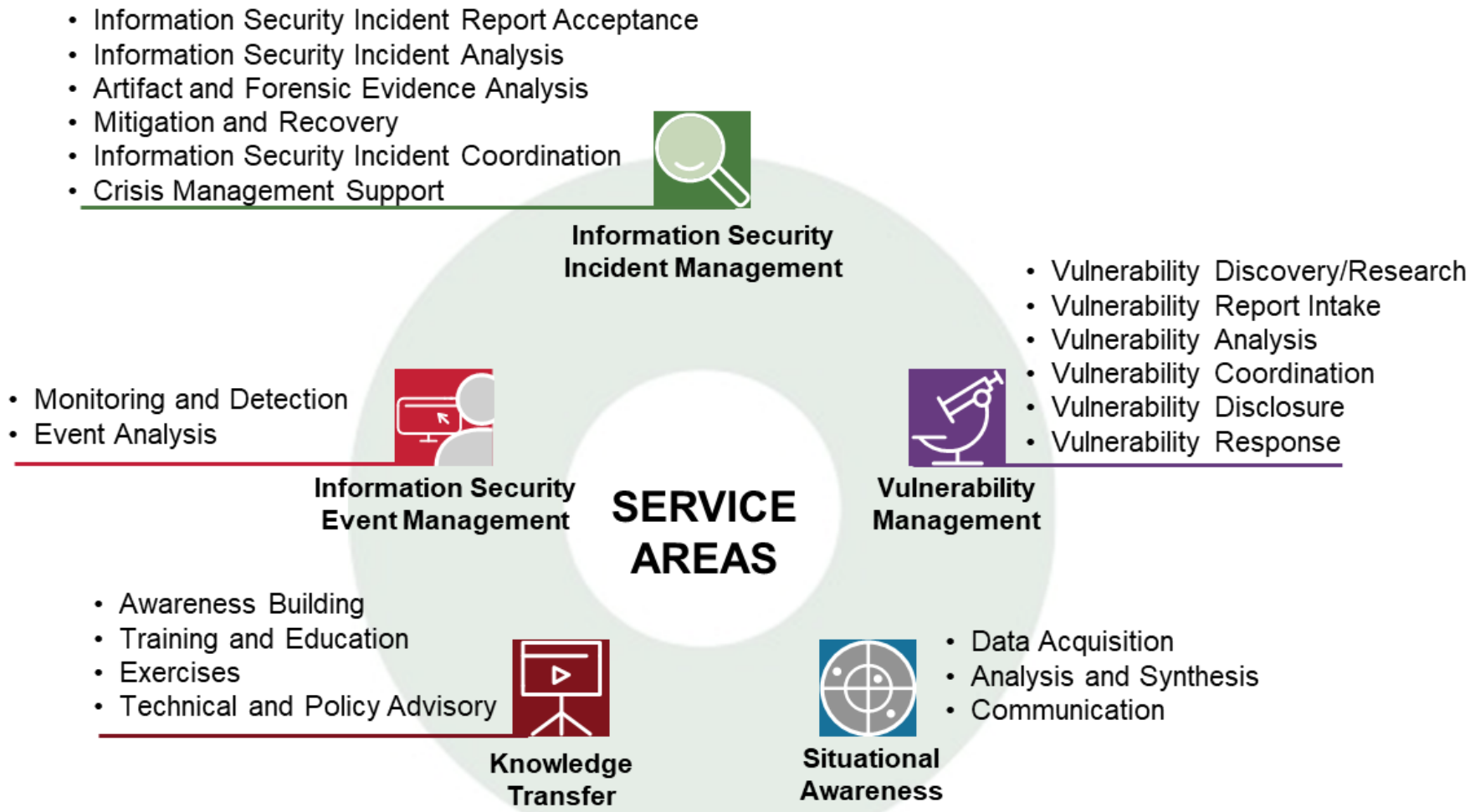
- The Internet
- Security Principles
- Security Vulnerabilities/ Weakness
- Risk
- Network Protocol
- Network Applications and Services
- Network Security Issues
- Host/System Security Issues
- Malicious Code
- Programming Skills

Incident Handling Skills

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

Standar Kompetensi Staf CSIRT

CSIRT SERVICES FRAMEWORK 2.1



REGULASI TIM TANGGAP INSIDEN

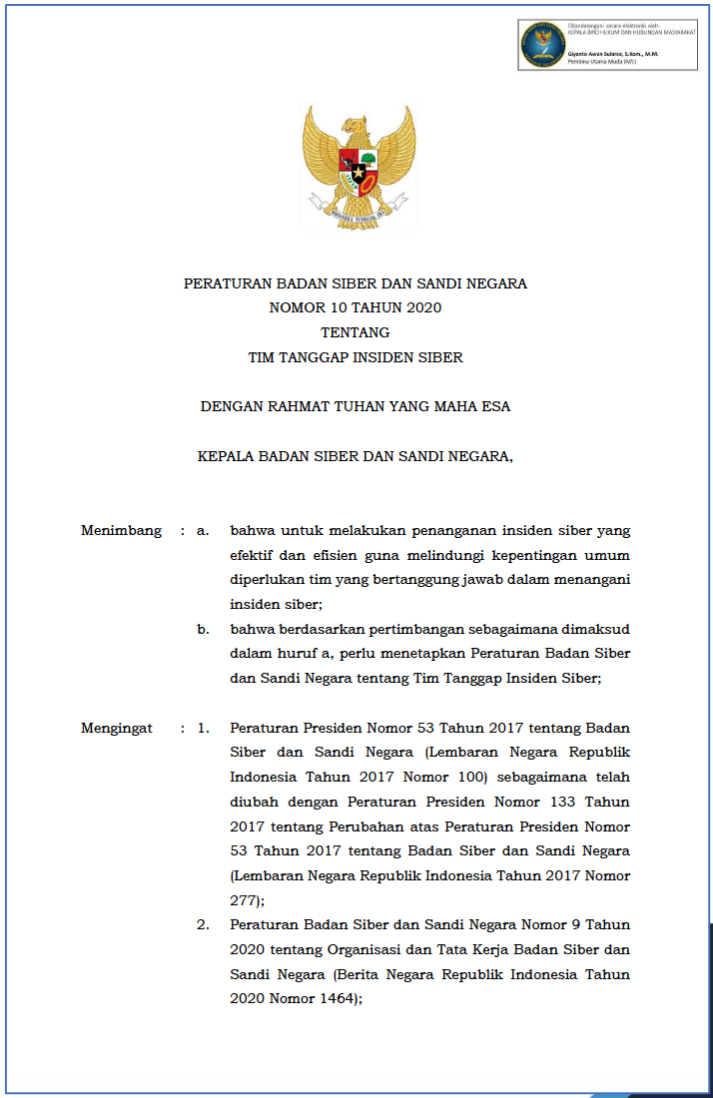
Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber.

04

Jenis TTIS

[Pasal 2]

- **Tim Tanggap Insiden Siber Nasional**
- **Tim Tanggap Insiden Siber Sektoral**
- **Tim Tanggap Insiden Siber Organisasi**
- **Tim Tanggap Insiden Siber Khusus**



PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 10 TAHUN 2020
TENTANG
TIM TANGGAP INSIDEN SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : a. bahwa untuk melakukan penanganan insiden siber yang efektif dan efisien guna melindungi kepentingan umum diperlukan tim yang bertanggung jawab dalam menangani insiden siber;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Tim Tanggap Insiden Siber;

Mengingat : 1. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 100) sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 277);

2. Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2020 Nomor 1464);

LAYANAN CSIRT

Jenis Layanan

Layanan utama

Terdiri atas:
a. Pemberian peringatan terkait keamanan siber; dan
b. Pengelolaan Insiden Siber.

[Pasal 13 ayat (1)]

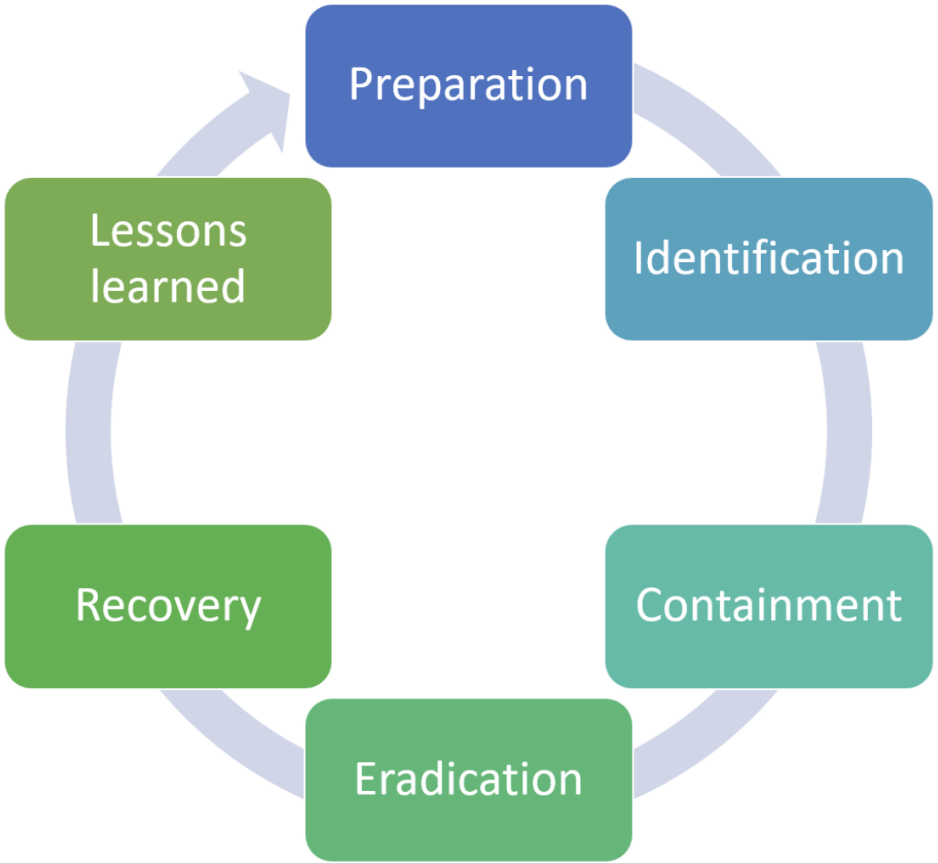
Layanan tambahan

Terdiri atas:
a. Penanganan kerentanan sistem elektronik; ***REAKTIF***
b. Penanganan artefak digital; ***REAKTIF***
c. Pemberitahuan hasil pengamatan potensi ancaman; ***PROAKTIF***
d. Pendeteksian serangan; ***PROAKTIF***
e. Analisis risiko keamanan siber; ***LAYANAN PENINGKATAN KESIAPAN PENANGANAN INSIDEN SIBER***
f. Konsultasi terkait kesiapan penanganan Insiden Siber; dan/atau ***LAYANAN PENINGKATAN KESIAPAN PENANGANAN INSIDEN SIBER***
g. Pembangunan kesadaran dan kepedulian terhadap keamanan siber. ***LAYANAN PENINGKATAN KESIAPAN PENANGANAN INSIDEN SIBER***

[Pasal 14 ayat (1)]

Sumber : Peraturan BSSN Nomor 10 Tahun 2020

FASE INSIDEN RESPON



- PERSIAPAN (PREPARATION) → Tim (internal, eksternal, role, kepemilikan sistem, penentuan layanan, jalur komunikasi alternative, partisipasi dalam program peningkatan kapasistas
- IDENTIFIKASI (IDENTIFICATION) → apakah insiden? Bagaimana ruang lingkupnya (dampak dan urgensi)? Identifikasi kategori insiden, tentukan SLA
- PENAHANAN (CONTAINMENT) → membatasi kerusakan dan mencegah terjadinya kerusakan lebih lanjut.
- PEMBERANTASAN (ERADICATION) → pemindahan dan pemulihan dari sistem yang terkena dampak
- RECOVERY (PEMULIHAN) → mengembalikan sistem yang terdampak insiden
- PEMBELAJARAN YANG DIDAPAT (LESSON LEARNED) → dokumentasi insiden dan tindakan penanganan yang dilakukan yang mungkin dapat dijadikan sebagai acuan apabila terjadi insiden yang serupa.

KESALAHAN UMUM DALAM CSIRT

- Tim CSIRT melakukan insiden response hingga perbaikan aplikasi
- Insiden terjadi karena kegagalan Tim CSIRT melindungi
- Sudah ada Tim CSIRT/Keamanan (semua masalah akan terselesaikan)
- Rencana tanggap insiden hanya digunakan saat terjadi insiden
- Tim CSIRT tidak membangun komunikasi dengan unit lain atau orang yang tepat
- Tidak ada data yang diperlukan Tim CSIRT untuk menganalisis insiden
- Skill dari anggota Tim CSIRT tidak dipelihara
- Pengguna di dalam organisasi tidak memahami perannya dalam keamanan
- Organisasi tidak memiliki identifikasi asset dan penilaian resiko keamanan terkait aset

EVALUASI OPERASIONAL CSIRT

- CSIRT perlu melakukan review terhadap dokumen RFC-2350
- Update website CSIRT
- Update kontak CSIRT
- Review pelaksanaan layanan
- Review sumber daya yang dimiliki (SDM, perangkat, sistem, form aduan, form penanganan)

```
1 Document Information
1.1 Date of Last Update
1.2 Distribution List for Notifications
1.3 Locations where this Document May Be Found

2 Contact Information
2.1 Name of Team
2.2 Address
2.3 Time Zone
2.4 Telephone Number
2.5 Facsimile Number
2.6 Other Telecommunication
2.7 Electronic Mail Address
2.8 Public Keys and Encryption Information
2.9 Team Members
2.10 Other information
2.11 Points of Customer Contact

3 Charter
3.1 Mission Statement
3.2 Constituency
3.3 Sponsorship and/or Affiliation
3.4 Authority

4 Policies
4.1 Types of Incident and Level of Support
4.2 Co-operation, Interaction and Disclosure of Information
4.3 Communication and Authentication

5 Services
5.1 Incident Response
5.2 Proactive activities

6 Incident Reporting Forms

7 Disclaimers
```

“(Ingatlah) Kechilafan Satu Orang Sahaja Tjukup Sudah Menjebabkan Keruntuhan Negara”

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