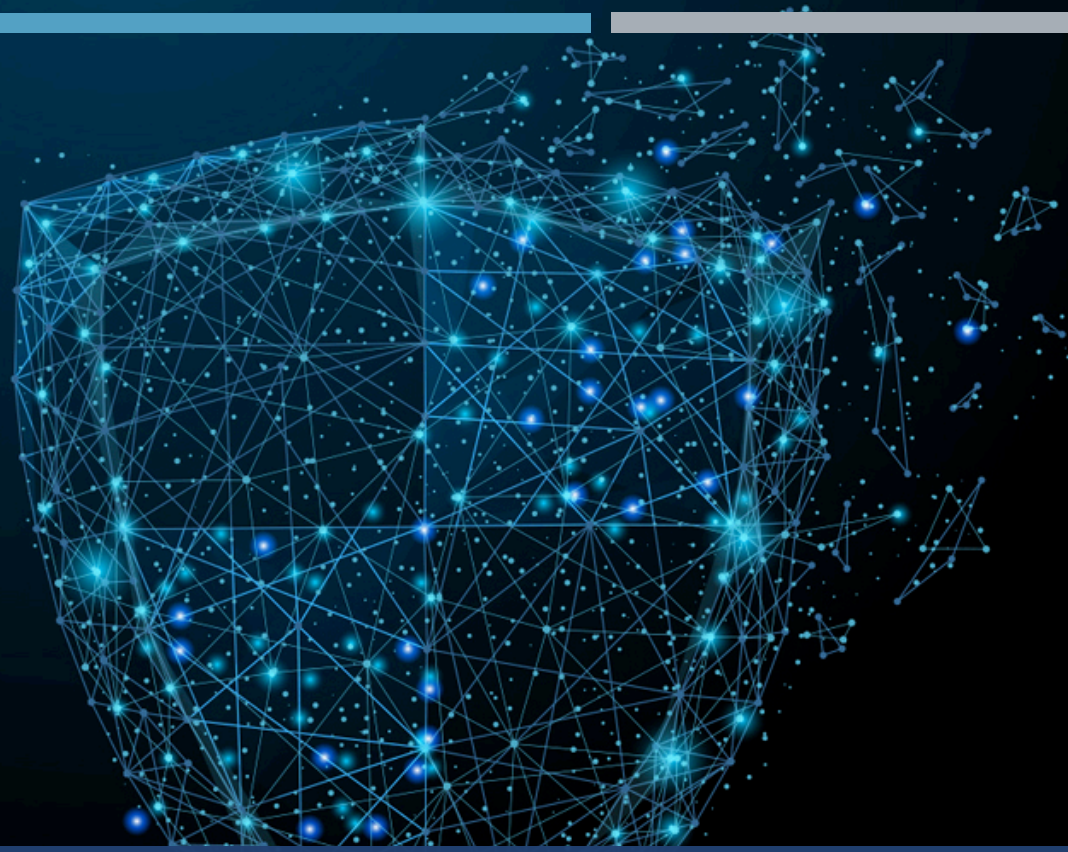
BADAN SIBER &
SANDI NEGARA



PENANGANAN INSIDEN YANG HANDAL

CASE : WEB DEFACEMENT DAN DDOS

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

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

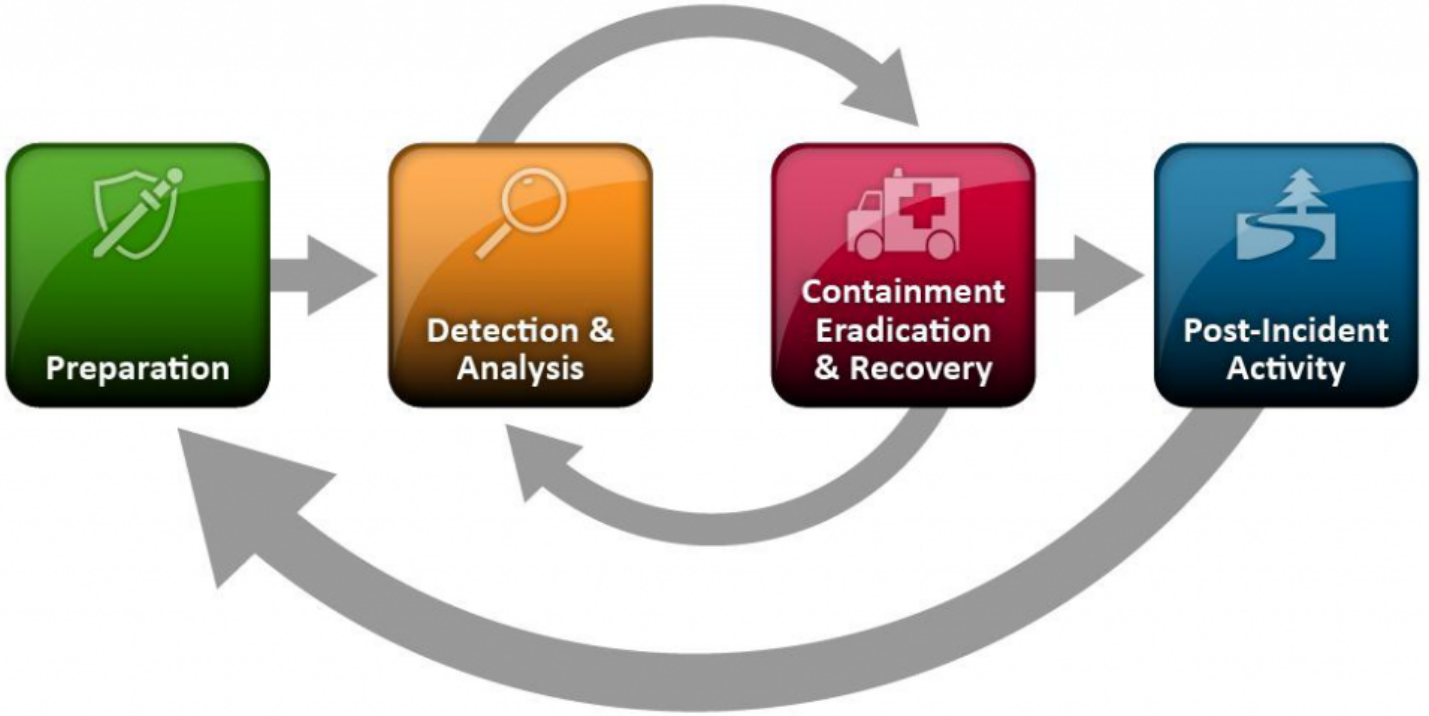
RESPON INSIDEN KEAMANAN SIBER

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



Sumber : NIST-SP800-61, Computer Security Incident Handling Guide

PREPARATION

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

DETECTION AND ANALYSIS

Yang dibutuhkan :

- Bukti Insiden
- Topologi Jaringan dan Sistem Komputer
- Kebijakan Keamanan (*Security Policy*)

Yang diinvestigasi :

- Awal Mula Serangan
- Dampak dan Keparahan Insiden *(Impact and Severity of Incident)*

BADAN SIBER & SANDI NEGARA

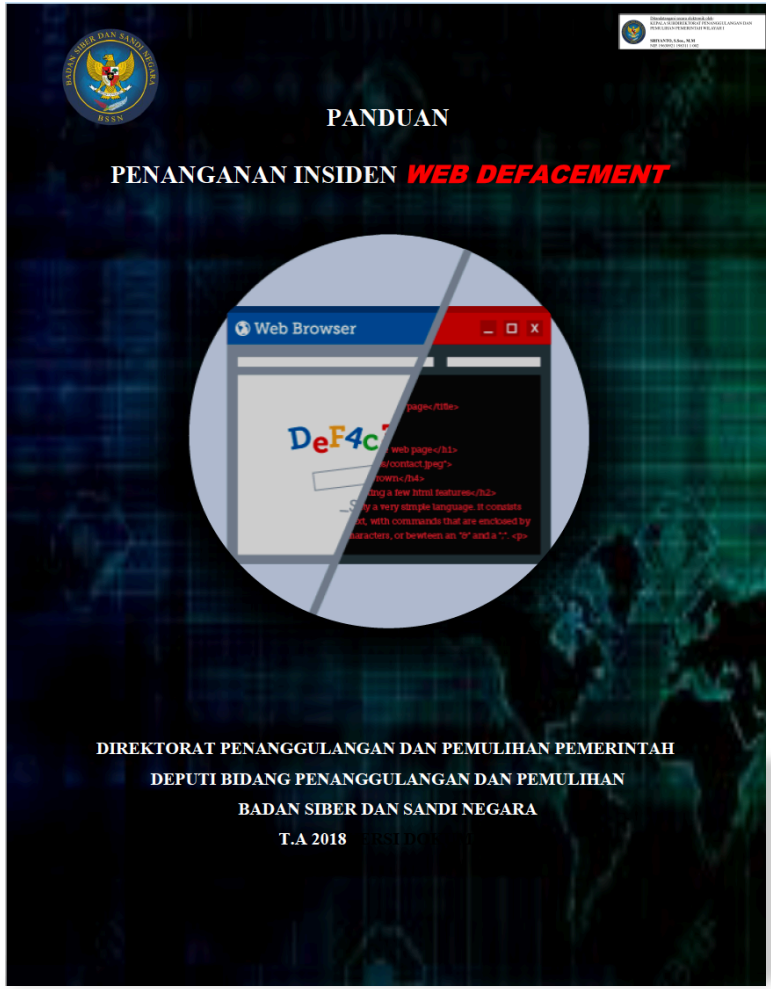
CONTAINMENT, ERADICATION AND RECOVERY

- Isolasi sistem terdampak
- Penghapusan artifak
- Perbaikan sistem terdampak
- Pemulihan

POST-INCIDENT

- *Lesson-Learned*
- *Vulnerability Assessment*
- *Hardening*

PANDUAN PENANGANAN INSIDEN *WEB DEFACEMENT*



1. Persiapan
2. Identifikasi dan Analisis
3. Mitigasi
4. Penghapusan Konten
5. Pemulihan
6. Tindak Lanjut

BADAN SIBER & SANDI NEGARA

PANDUAN PENANGANAN INSIDEN *WEB DEFACEMENT*

1. Persiapan
   a. Pembentukan Tim Penanganan Insiden (CSIRT);
   b. Menyiapkan dokumen yang dibutuhkan : SOP, Form Penanganan Insiden, Form *Chain of Custody*, topologi *network*, dokumentasi dari sistem operasi, aplikasi, protokol, anti virus;
   c. Lakukan koordinasi dengan tim operasional TI, CSIRT
   d. Menyimpan bukti insiden : *screenshot, log* dari *server*
   e. Menentukan tempat/ruangan untuk menangani insiden
   f. Menyiapkan *tools* dan media yang dibutuhkan untuk menanganani insiden

PANDUAN PENANGANAN INSIDEN *WEB DEFACEMENT*

2. Identifikasi dan Analisis
    a. Memeriksa file-file yang bersifat statis;
    b. Memeriksa semua *log* file : *access log, error log, database log, auth log;*
    c. Memeriksa folder pada website yang bersifat publik;
    d. Memeriksa kode SQL yang digunakan pada web aplikasi;
    e. Memeriksa versi setiap aplikasi/*library* yang digunakan;
    f. Memeriksa koneksi yang terhubung ke *server;*
    g. Memeriksa layanan/*service* yang sedang berjalan dan *service* otomatis (cronjob);
    h. Memriksa *port* yang terbuka,
    i. Memeriksa *last login;*
    j. Memeriksa *history*..

PANDUAN PENANGANAN INSIDEN *WEB DEFACEMENT*

3. Mitigasi

   a. Pembangunan *website* sementara agar publikasi informasi tetap berjalan;

   b. Lakukan *backup* sistem untuk keperluan forensik;

   c. Pembatasan akses terhadap sumber serangan : alamat IP, *port*, *akun*.

PANDUAN PENANGANAN INSIDEN *WEB DEFACEMENT*

4. Penghapusan Konten

   a. Menghapus file *malicious;*

   b. Meng-*uninstall* aplikasi *malicious*..

PANDUAN PENANGANAN INSIDEN *WEB DEFACEMENT*

5. Pemulihan

a. Mengaktifkan *file-file* yang telah di-*backup*

b. Melakukan *upgrade/update/patch* semua aplikasi yang diguakan di *web server;*

c. Lakukan *automatic updates* pada setiap aplikasi yang digunakan;

d. Lakukan pembaruan seluruh akun;

e. Lakukan *hardening* server.

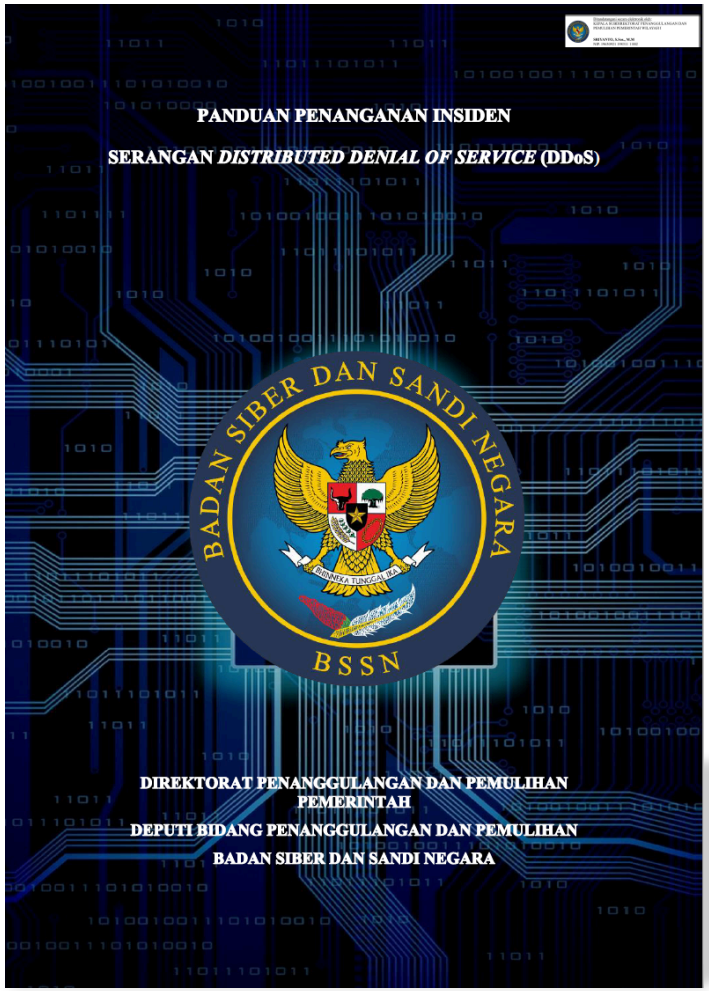
BADAN SIBER & SANDI NEGARA

PANDUAN PENANGANAN INSIDEN *WEB DEFACEMENT*

6. Tindak Lanjut

   a. Lakukan uji keamanan *web server* dan aplikasi;
   b. Memetakan kerentanan yang ditemukan;
   c. Membuat semua dokumentasi dan laporan terkait;
   d. Menuliskan *tools* yang digunakan;
   e. Menuliskan bukti-bukti yang ditemukan;
   f. Memberikan analisis dan penjelasan apa yang harus dilakukan (*lesson learned incident*);
   g. Membuat evaluasi dan rekomendasi.

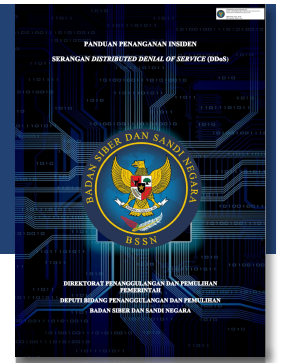
PANDUAN PENANGANAN INSIDEN DDOS



1. Persiapan
2. Identifikasi dan Analisis
3. *Containment*
4. Penghapusan Konten (*Eradication*)
5. Pemulihan
6. Tindak Lanjut

BADAN SIBER & SANDI NEGARA

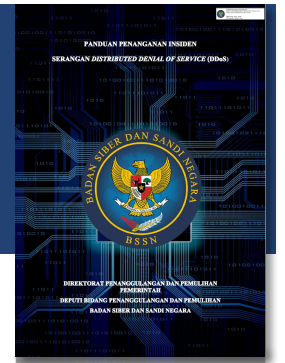
PANDUAN PENANGANAN INSIDEN DDOS



I. Persiapan

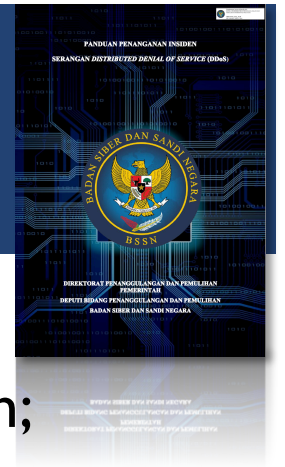
a. Pembentukan Tim Penanganan Insiden (CSIRT);
b. Membangun kontak dengan ISP;
c. Menyiapkan dokumen yang dibutuhkan : SOP, Form Penanganan Insiden, Form *Chain of Custody*, topologi *network*, dokumentasi dari sistem operasi, aplikasi, protokol, anti virus;
d. Menyiapkan yang dibutuhkan untuk penanganan insiden;
e. Menyiapkan desain jaringan secara redundan;
f. Melakukan *backup* secara berkala.

PANDUAN PENANGANAN INSIDEN DDOS



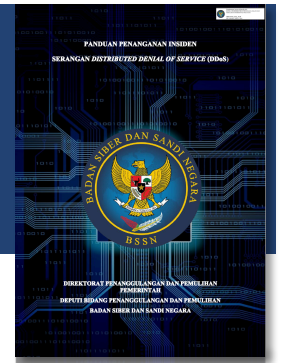
2. Identifikasi dan Analisis
    a. Mengetahui perilaku "normal" dari lalu lintas jaringan, penggunaan CPU, dan penggunaan *memory;*
    b. Mengidentifikasi komponen infrastruktur yang terkena dampak;
    c. Berkoordinasi dengan pihak terkait;
    d. Memeriksa lalu lintas jaringan;
    e. Menganalisis file *log* yang tersedia;
    f. Menentukan dampak yang terjadi;

PANDUAN PENANGANAN INSIDEN DDOS



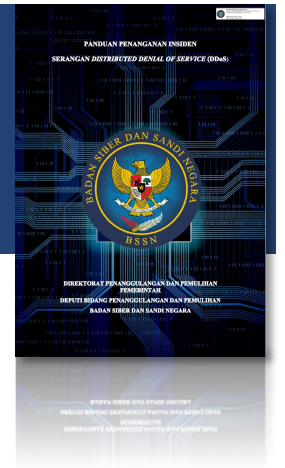
3. *Containment*
    a. Jika sumber *bottleneck* dari fitur aplikasi, maka aplikasi dapat dinonaktifkan;
    b. Jika *bottleneck* berada di ISP, maka bisa berkoordinasi untuk dilakukan *filtering;*
    c. Merelokasi target ke alamat IP lain, jika *host* menjadi target serangan;
    d. Mengontrol lalu lintas dana dengan menghentikan koneksi atau proses yang tidak diinginkan;
    e. Melakukan *filter* sesuai dengan karakteristik serangan;
    f. Menerapkan *rate limit*;
    g. Jika memungkinkan blokir lalu lintas yang terhubung ke jaringan.

PANDUAN PENANGANAN INSIDEN DDOS



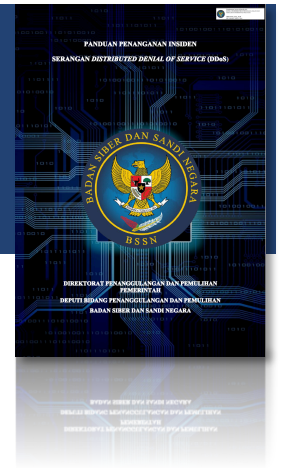
4. *Eradication*
    a. Pemblokiran jaringan;
    b. Pemfilteran;
    c. *Traffic-scrubbing/shinkhole/clean-pipe;*
    d. *Blackhole routing.*

PANDUAN PENANGANAN INSIDEN DDOS



5. *Recovery*
    a. Memastikan serangan DDOS selesai dan layanan bisa berfungsi kembali;
    b. Jaringan telah bekerja dengan normal;
    c. Layanan yang terkena dampak bisa berfungsi normal;
    d. Infrastruktur telah bekerja dengan normal;
    e. Memulai layanan, aplikasi, dan modul yang ditangguhkan;
    f. Mengembalikan ke jaringan asli.

PANDUAN PENANGANAN INSIDEN DDOS



6. Tindak Lanjut
    a. Membuat dokumentasi dan laporan terkait;
    b. Evaluasi efektivitas respon;
    c. Menyempurnakan langkah-langkah respon;
    d. Mencatat *tools* yang digunakan;
    e. Mendokumentasikan bukti-bukti yang ditemukan;
    f. Memberikan analisis dan penjelasan apa yang harus dilakukan;
    g. Membuat evaluasi den rekomendasi.

BADAN SIBER &
SANDI NEGARA

TERIMA KASIH