BADAN SIBER & SANDI NEGARA

PENYELENGGARAAN PENANGGULANGAN DAN PEMULIHAN INSIDEN SIBER

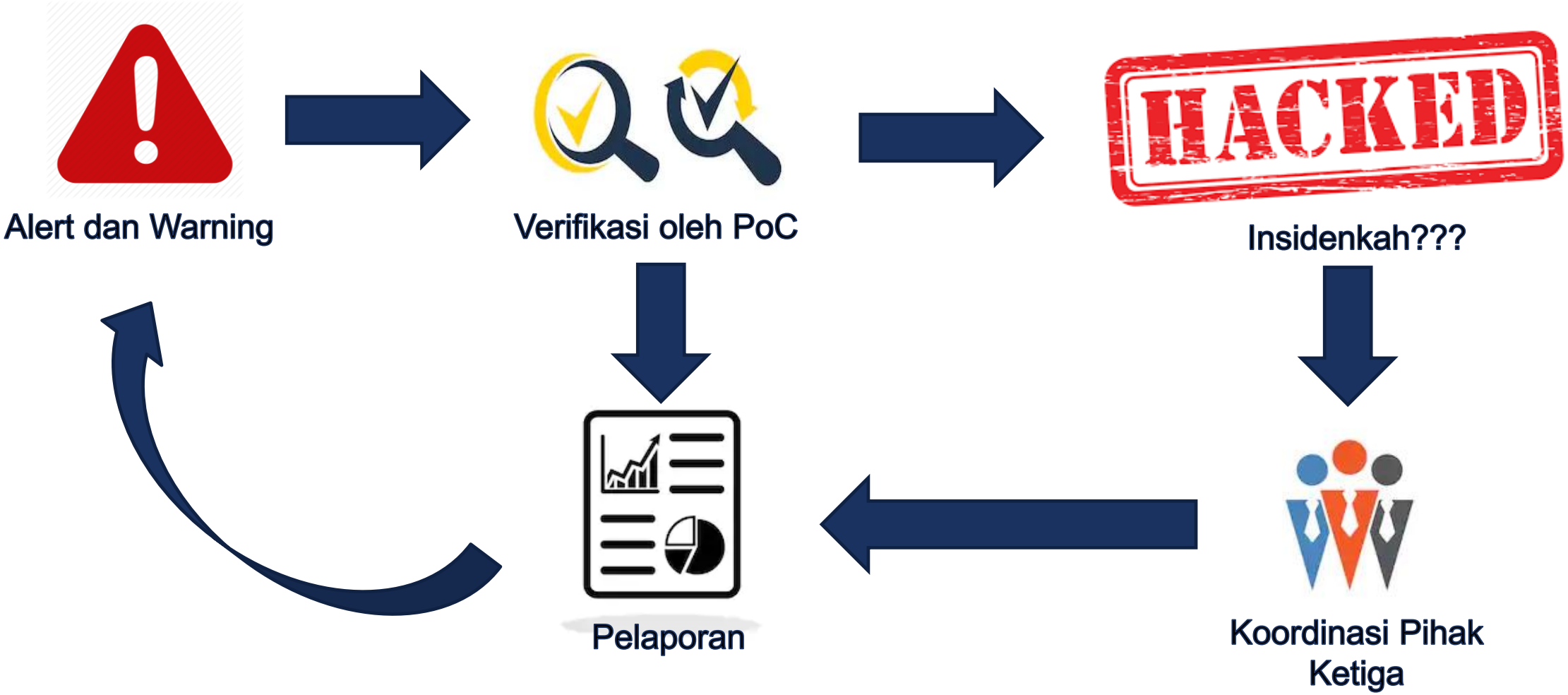
DIREKTORAT PENANGGULANGAN DAN PEMULIHAN PEMERINTAH,
DEPUTI BIDANG PENANGGULANGAN DAN PEMULIHAN
BSSN

PENYELENGGARAAN GULIH CSIRT

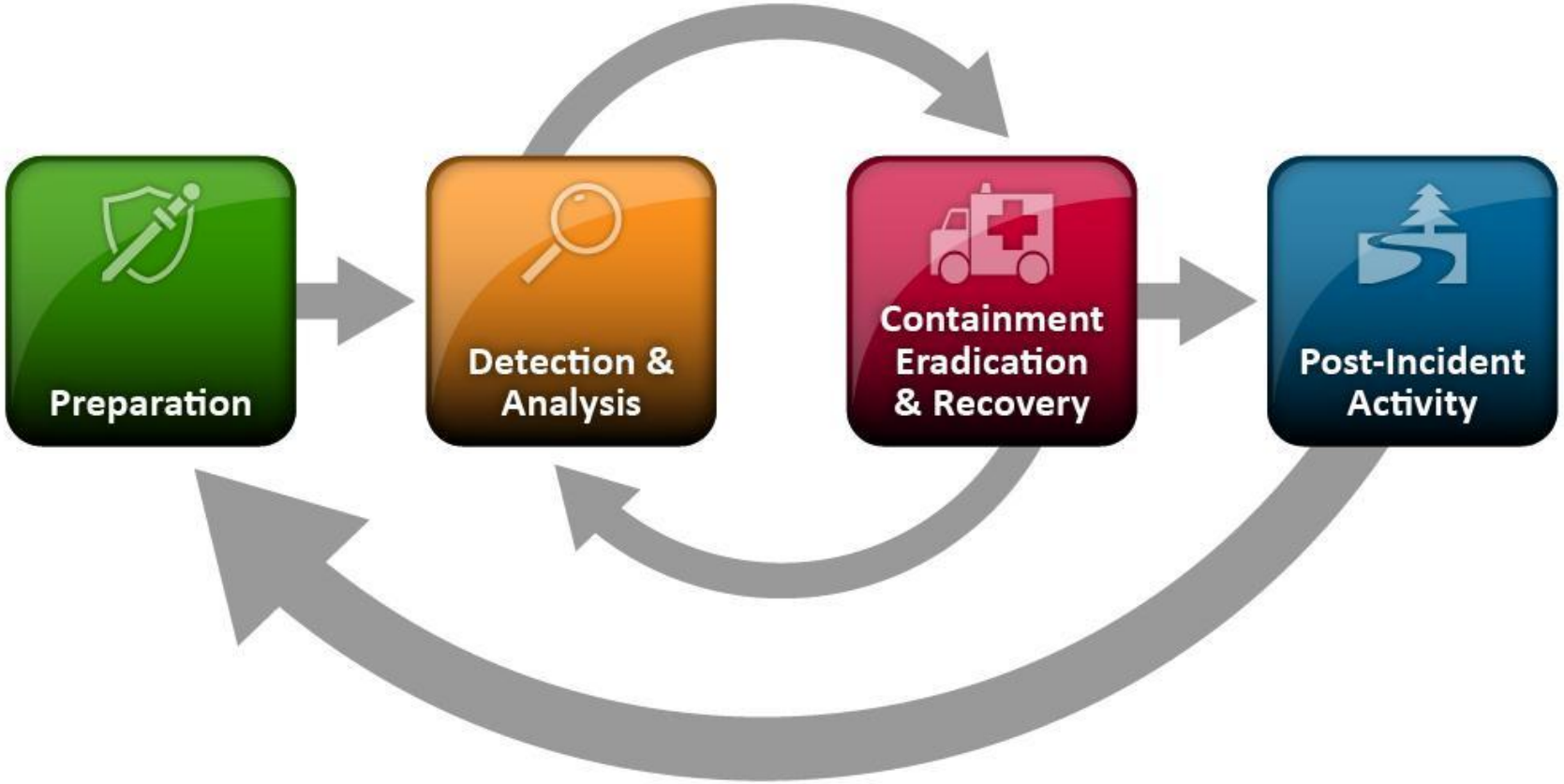
- Model CSIRT Koordinasi
- Model CSIRT Tim Internal
- Penyelenggaraan CSIRT yang Efektif

BADAN SIBER & SANDI NEGARA

MODEL CSIRT KOORDINASI



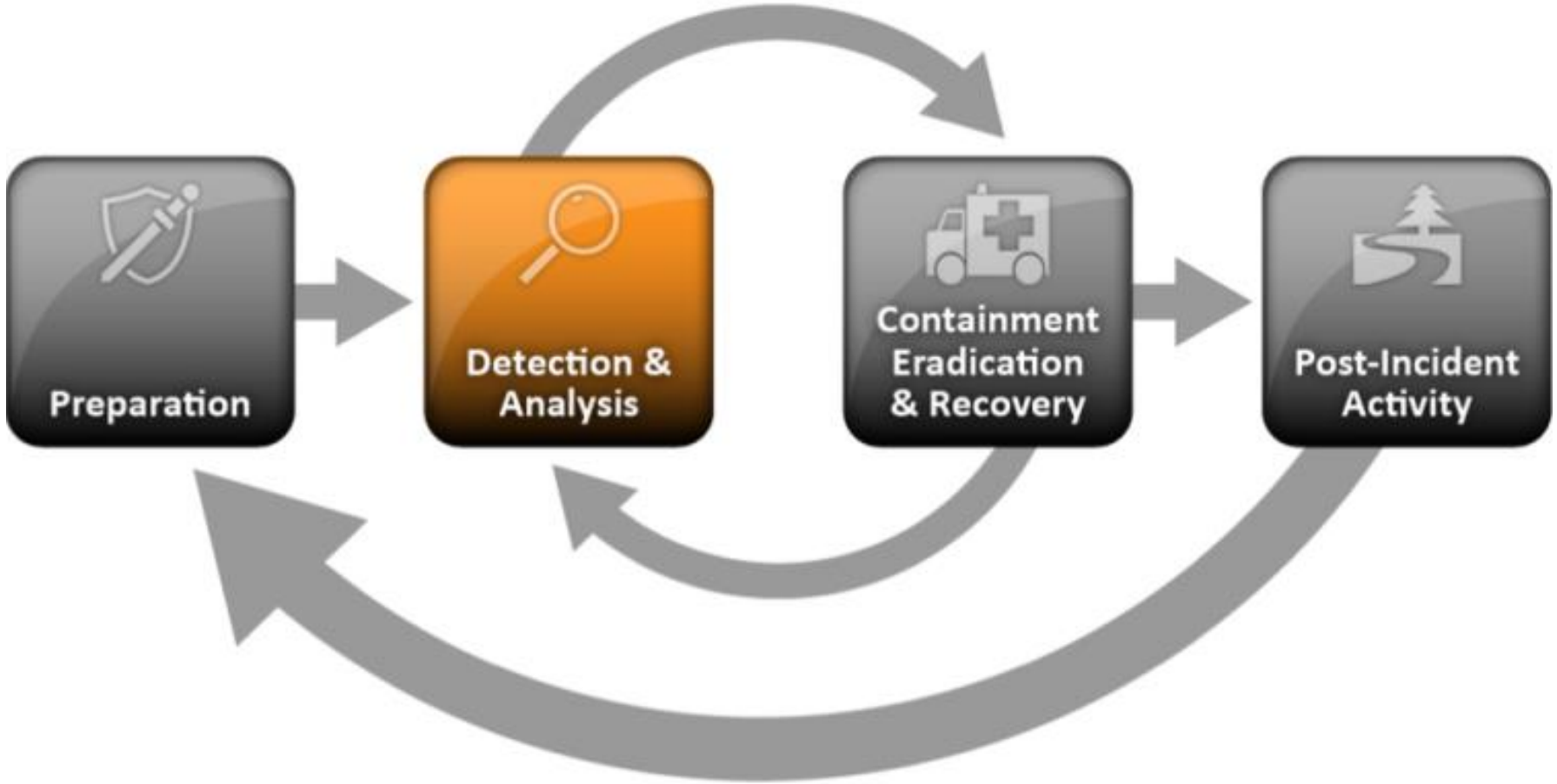
MODEL CSIRT DENGAN TIM INTERNAL



Sumber : NIST.SP.800-61r2 (Computer Security Incident Handling Guide

PREPARATION

- Penentuan Kebijakan
- Penentuan *Response Plan/Strategy*
- Rencana alur komunikasi
- Dokumentasi
  - Log, Bukti Insiden, Dokumen Pendukung lainnya
- Tim Penanggulangan Insiden
- Access Control
- Tools
  - Vulnerability Scanning Tools, Forensic Tools, Malware Analisis Tools


Preparation
Detection &
Analysis
Containment
Eradication
& Recovery
Post-Incident
Activity

DETECTION & ANALYSIS

- Adalah tahapan mendeteksi dan menganalisa apakah benar terjadi insiden, seperti apa insiden yang terjadi (5 W + 1 H) dan sampai sejauh mana dampak insiden tersebut.
- Hal yang perlu dilakukan pada tahap ini yaitu mengumpulkan dan menganalisis *log files*, error message dan sumber lain seperti hasil *intrusion detection systems* dan *firewalls*

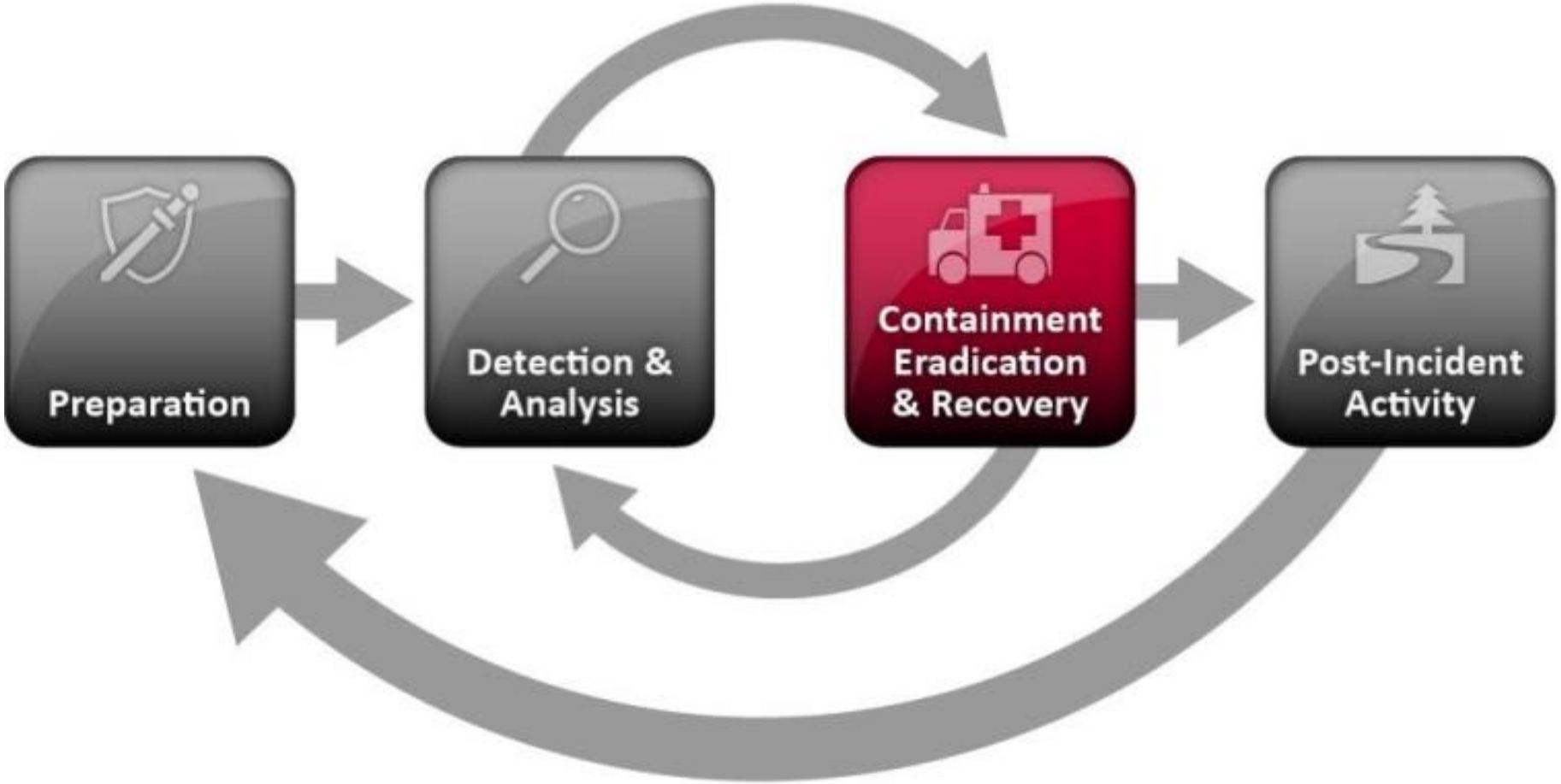
DETECTION & ANALYSIS

Detection

- Monitoring bandwidth
- Monitoring jaringan
- Memahami normal activity
- Alert system
- Intrusion Detection System

Analysis

- Log Analysis
- Service Analysis
- Web Application Directory
- Network Connection
- Database


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Containment	Eradication	Recovery
Menjaga dampak dari sebuah insiden agar tidak tersebar secara luas. Mengisolasi sebuah segmen jaringan yang terinfeksi oleh serangan sehingga tidak mengganggu alur pertukaran data dalam seluruh sistem.	Pembersihan sistem elektronik yang terkena serangan, baik malware, bakcdoor, malicious file lainnya. Perlu dilakukan imaging / back-up terhadap sistem untuk kepentingan analisis forensik digital dan proses pendokumentasian	Mengembalikan sistem yang terinfeksi serangan kembali sistem keseluruhan sebuah organisasi setelah sebelumnya diisolasi

CONTAINMENT TECHNIQUE

Short Containment

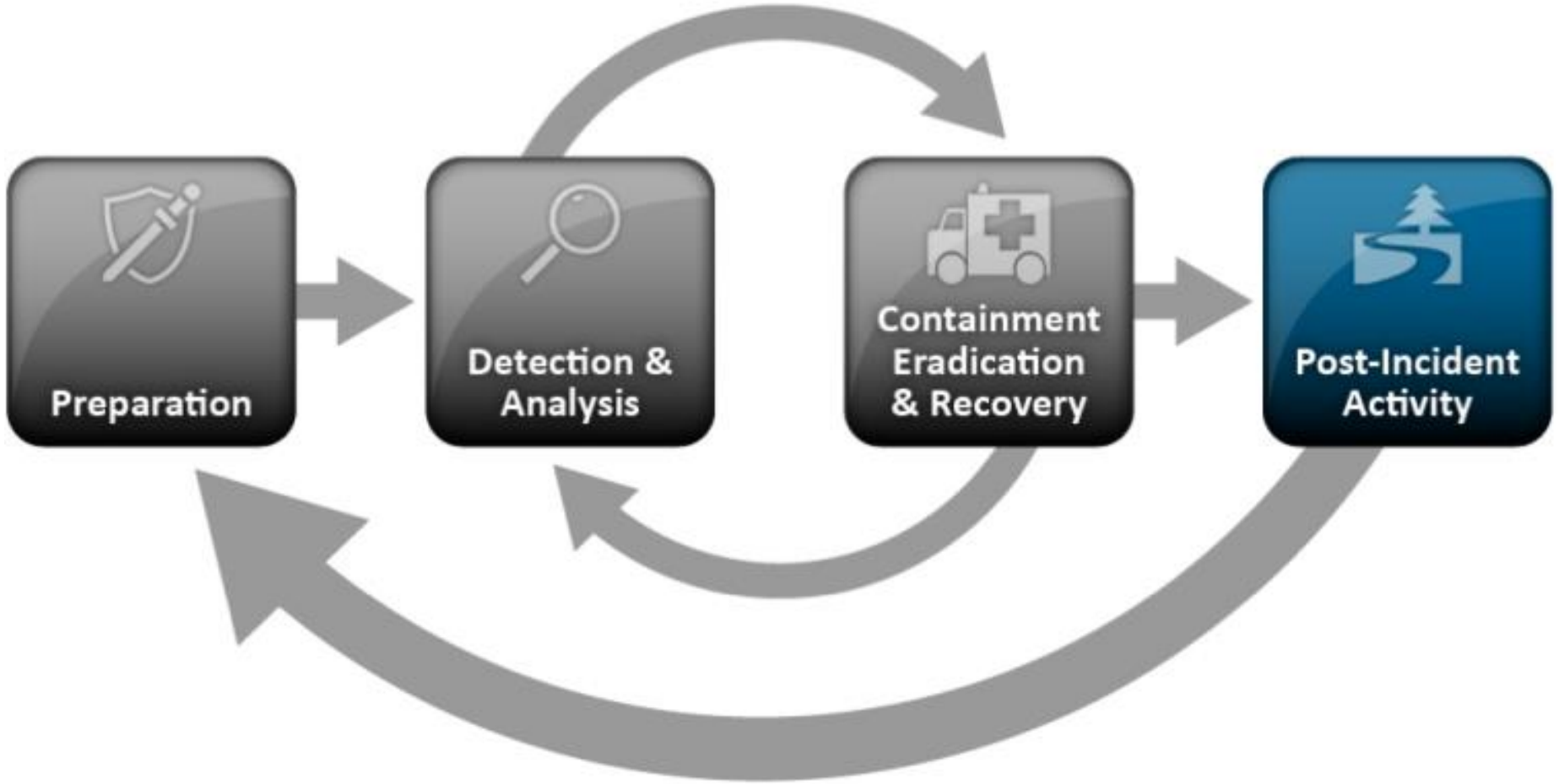
- Langkah awal mengurangi penyebaran dampak
- Mengisolasi sebuah segmen jaringan yang terinfeksi oleh serangan
- Sehingga tidak mengganggu alur pertukaran data dalam seluruh sistem

Backup

- Imaging (Bit per bit copy)
- Application dan Database backup
- Digital forensic

Long Containment

- Partial backup
- Identifikasi dan Analisis Root Cause
- Backdoor analysis


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

POST-INCIDENT ACTIVITY

- Tahap ini bertujuan untuk melengkapi dokumentasi yang belum rampung dikerjakan saat proses penanggulangan insiden.
- Dari dokumentasi ini, diharapkan organisasi dapat mengambil pelajaran dari insiden yang terjadi untuk melakukan perbaikan dalam tim CSIRT
- Melakukan *analysis vulnerability* terhadap sistem elektronik
- Melakukan perbaikan dan *hardening* terhadap sistem elektronik
- Melakukan monitoring dan observasi terhadap sistem elektronik tersebut setelah diaktifkan kembali

CON'T

- Adapun poin-poin yang sebaiknya disajikan dalam dokumentasi adalah:
  - kapan insiden terjadi dan oleh siapa insiden berhasil terdeteksi;
  - lingkup insiden yang terjadi;
  - bagaimana insiden tersebut ditangani/ditanggulangi;
  - tindakan yang dilakukan ketika melakukan proses *recovery*;
  - area/lingkup kerja yang efektif dikerjakan oleh tim CSIRT dalam menangani insiden;
  - area/lingkup kerja yang membutuhkan peningkatan kinerja tim CSIRT

PENYELENGGARAAN CSIRT YANG EFEKTIF

1. Pembagian peran dan tanggungjawab yang jelas
2. SOP yang lengkap dan jelas dan mengarah ke bagaimana menangani insiden dengan cepat
3. Membangun kolaborasi dengan pemilik aset
4. Alur komunikasi yang baik
5. Melakukan drill test / simulasi secara berkesinambungan
6. Dokumentasi / Laporan yang baik serta ditindaklanjuti

BADAN SIBER &
SANDI NEGARA

TERIMA KASIH