BADAN SIBER &
SANDI NEGARA

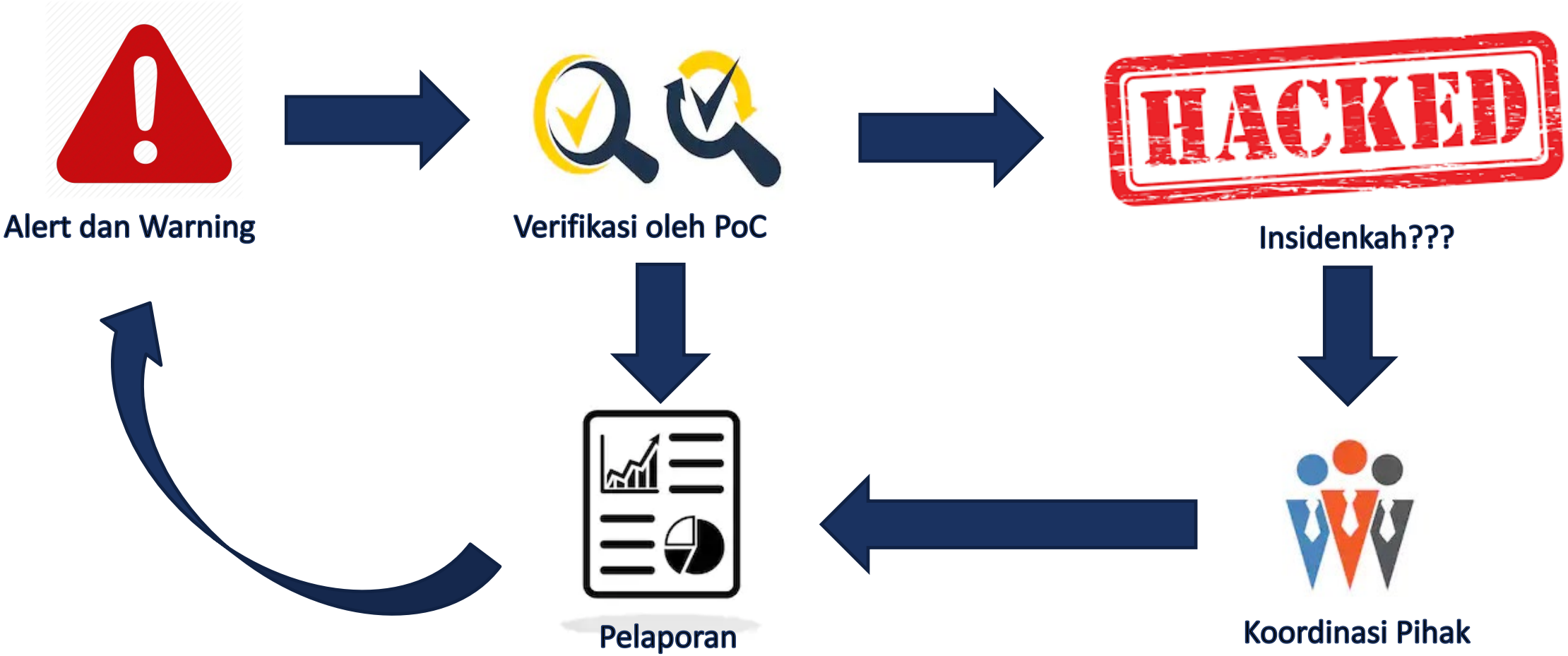
PENYELENGGARAAN PENANGGULANGAN DAN PEMULIHAN INSIDEN SIBER

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

PENYELENGGARAAN GULIH CSIRT

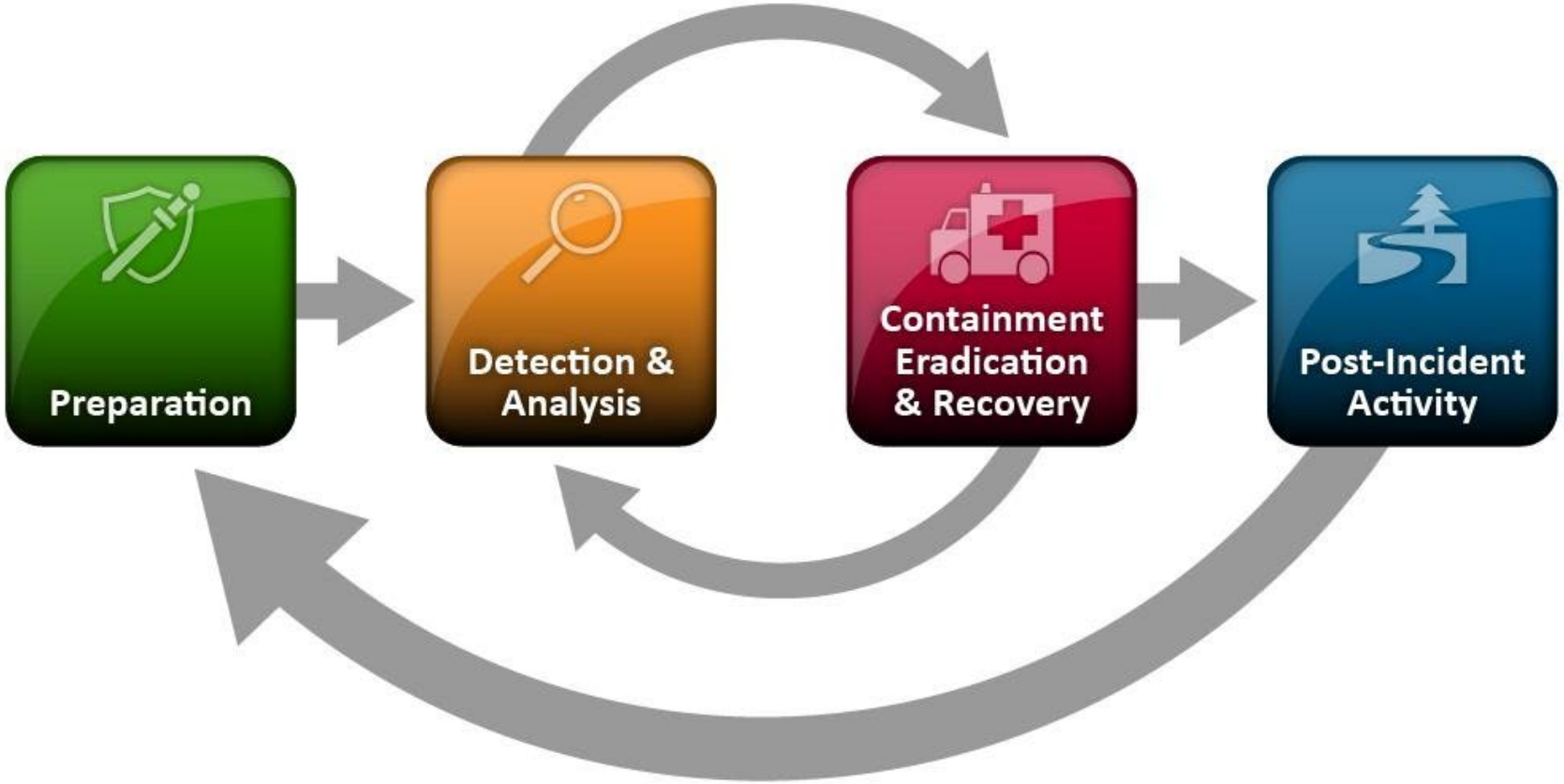
- Model CSIRT Koordinasi
- Model CSIRT Tim Internal
- Penyelenggaraan CSIRT yang Efektif

MODEL CSIRT KOORDINASI



BADAN SIBER & SANDI NEGARA

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
- Tools
  - Vulnerability Scanning Tools, Forensic Tools, Malware Analisis Tools

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*

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

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

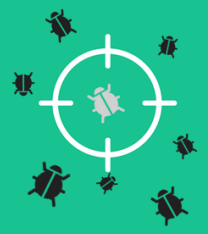
PENYELENGGARAAN CSIRT YANG EFEKTIF dengan mekanisme Triage Incident

- Triage Incident adalah proses memilah incident berdasarkan tingkat keparahan yang diakibatkan oleh incident tersebut untuk menentukan tindakan apa saja yang harus dilakukan dan mana yang menjadi prioritas.
  - Identifikasi
  - Pemetaan
  - Penghapusan

TRIAGE INCIDENT

3 Steps for Effective Information Security Event Triage

A method to help you respond faster and with better accuracy to security events.



STEP 1: IDENTIFY

Start by collecting data, and identifying artifacts in the incident.

Likely tasks include:

- Retrieve logs
- Extract any artifacts: IPs, URLs, malware, etc.
- Look up reputations
- Detonate files in a sandbox

The goal is to identify any compromised or infected endpoints

STEP 2: MAP

With key indicators of compromise, piece the artifacts together

Likely tasks include:

- Review audit logs
- Playback monitoring recordings
- Draw a timeline of events

The goal is to determine how the attacker got in, where they went, and what they were looking to retrieve

STEP 3: ERADICATE

Now that you've identified any affected or compromised areas, it's time to remove the threat

Likely tasks include:

- Remove malware
- Delete infected assets
- Restore the system from backup

The goal is to is to eradicate any malicious contents, so the attacker no longer poses a threat in this instance

PERMASALAHAN PENANGGULANGAN INSIDEN

- Mengandalkan tools untuk melakukan pemantauan adanya serangan siber
  1. Apakah ini serangan yang sebenarnya? (Identifikasi)
  2. Apakah serangannya berhasil? (Identifikasi)
  3. Aset apa lagi yang juga *compromised*? (Pemetaan)
  4. Kegiatan apa yang dilakukan penyerang? (Pemetaan)
  5. Bagaimana seharusnya organisasi saya menanggapi serangan ini? (Penghapusan)

APAKAH INI SERANGAN YANG SEBENARNYA?

- Dapat dilihat apakan peringatan yang diberikan berupa *false positive* atau memang sebuah serangan terjadi.
- Untuk mengetahui apakah merupakan *false positive* atau bukan dapat dilakukan analisa secara langsung dan mengidentifikasi informasi lain

APAKAH SERANGANNYA BERHASIL?

- Jika terdapat IDS biasanya akan terlihat bahwa ada upaya serangan yang dilakukan namun tidak berhasil.
- Namun sebaiknya lebih dilakukan analisa yang mendalam terkait serangan yang dilakukan untuk mengidentifikasi apakah memang sudah terjadi serangan tersebut.

ASET APA LAGI YANG JUGA *COMPROMISED*?

- Apabila memang serangan berhasil maka perlu mendapatkan informasi dasar dan perencanaan yang matang terkait insiden yang terjadi
- Menyusun aset aset yang dapat berdampak dari serangan yang terjadi (komputer, perangkat jaringan, akun, email, file dll.

KEGIATAN APA YANG DILAKUKAN PENYERANG?

- Dapat dilihat dengan melakukan analisis berdasarkan waktu sejak penyerang melakukan serangan
- Mendapatkan log untuk mengetahui proses serangan
- Diketahui apakah ada backdoor yang ditanam sampai ke data rahasia yang berhasil didapatkan

BAGAIMANA SEHARUSNYA ORGANISASI SAYA MENANGGAPI SERANGAN INI?

- Setelah disusun daftar aset yang mungkin *compromised* dan waktu kejadian, selanjutnya proses respon insiden yang akan dilakukan.
- Sudah mengetahui alur serangan maka strategi awal yaitu memutus akses penyerang ke aset yang *compromised*, melakukan pemulihan aset dengan memprioritaskan respon berdasarkan asset yang bernilai tinggi
- Melakukan penghapusan backdoor atau file file yang mencurigakan
- Proses harus dilakukan secara cepat untuk meminimalkan kerusakan sistem

BADAN SIBER &
SANDI NEGARA

TERIMA KASIH