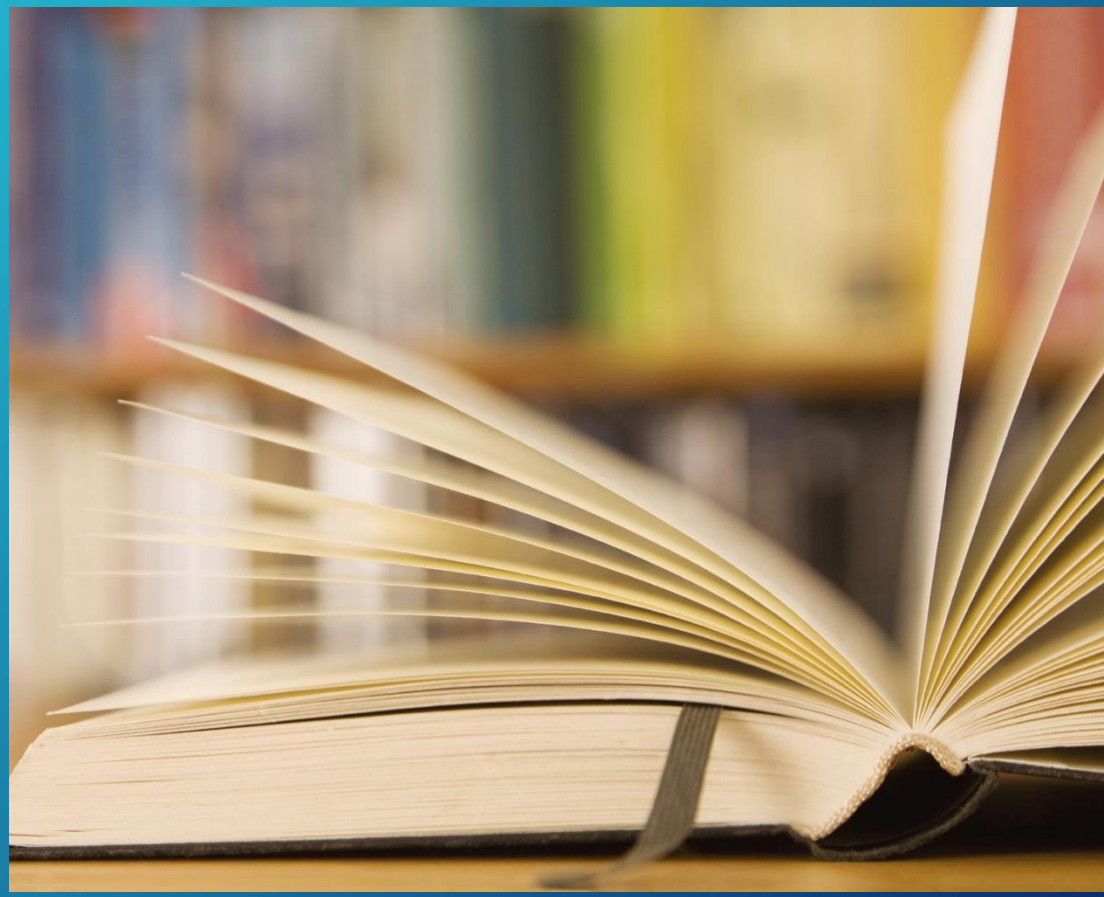
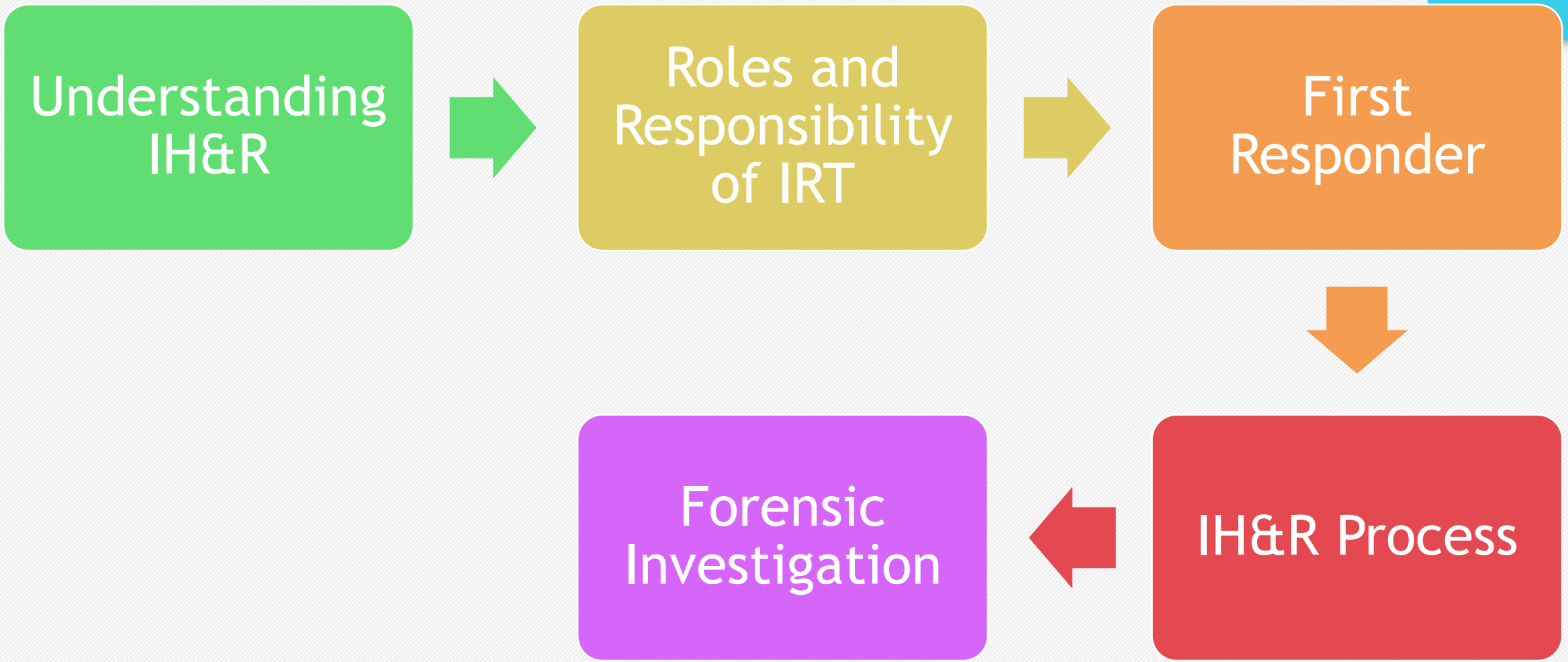
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

INCIDENT RESPONSE



Keamanan Sistem Informasi – Aditya Putra, ST., MT.

Agenda


Understanding IH&R
Roles and Responsibility of IRT
First Responder
IH&R Process
Forensic Investigation

IH&R - Incident Handling and Response

KONSEP

- **IH&R** adalah proses pengambilan Langkah yang teroganisir dan bertahap Ketika menghadapai adanya security incident
- Langkah-Langkah yang dimaksud dimulai dari Ketika insiden pertama kali disadari dan dilaporkan
- Proses IH&R bisa jadi berbeda tiap organisasi tergantung prosedur/aturan masing-masing
- Tim yang menangani security incident menjalankan rangkaian incident response plan disebut dengan **Incident Response Team (IRT)** baik internal maupun eksternal

IRT - Members and Roles

Management	• Pemilik kepemimpinan dan Pengambil kebijakan
Info SecTeam	• Berpengalaman dalam menemukan dan melokalisir insiden
IT Staff	• Staf support sehari-hari di bidang IT seperti network admin
Physical Security Staff	• Petugas pengamanan fisik
Attorney	• Mengurus keperluan di bidang legal dan hukum
HR Representative	• HR mengurus isu kepegawaian yang terkait dengan insiden
PR Specialist	• Berurusan dengan pihak eksternal organisasi setelah insiden terjadi
Financial Auditor	• Mengevaluasi potensi/dampak dari terjadinya insiden
IR Officer	• Melakukan semua aksi dan fungsi teknis IRT
IR Manager	• Penerima alert IR pertama dan memimpin tim IRT di semua aktivitasnya
IR Assessment Team	• Melakukan severity assessment untuk mengklasifikasikan tingkatan insiden
IR Custodians	• Melakukan remediasi dan resolusi pasca terjadinya insiden

FIRST RESPONDER – Penanggap Pertama

- First Responder atau Penanggap Pertama adalah orang yang pertama kali dating ke lokasi insiden dan mengabarkan notifikasi insiden kepada tim IRT
- Mereka bisa jadi end-user, network administrator, petugas penegak hukum, atau petugas investigasi
- Berikut yang perlu dilakukan oleh First Responder

Melaporkan Insiden	Memberikan notifikasi kepada Management dan IRT	Sterilisasi/Lokalisir Intrusi	Mengidentifikasi Tempat Kejadian Perkara (TKP)	Mengumpulan bukti dan informasi terkait insiden
Melindungi TKP	Mendokumentasikan semua temuan	Menjaga bukti-bukti yang temporer atau fragile	Mengamankan dan mengirimkan bukti elektronik	

Peran FIRST RESPONDER

NETWORK ADMINISTRATOR

- Network Administrator menghabiskan sebagian besar waktunya di lingkungan IT dan jaringan, sehingga ia sangat familiar dan memahami dengan baik trafik jaringannya, performance, kegunaan, topologi, lokasi setiap sistem, policy, dll
- Peran Network Administrator sangat penting sebagai First Responder Ketika terjadi insiden. Mereka dapat mendeteksi sumber insiden dan sistem mana yang terdampak dari insiden tersebut
- Jika mereka tidak aware prosedur dari insiden respon, maka akan memperlama waktu insiden respon yang tentu berakibat dengan bertambahnya potensi kerugian dan dampak yang meluas

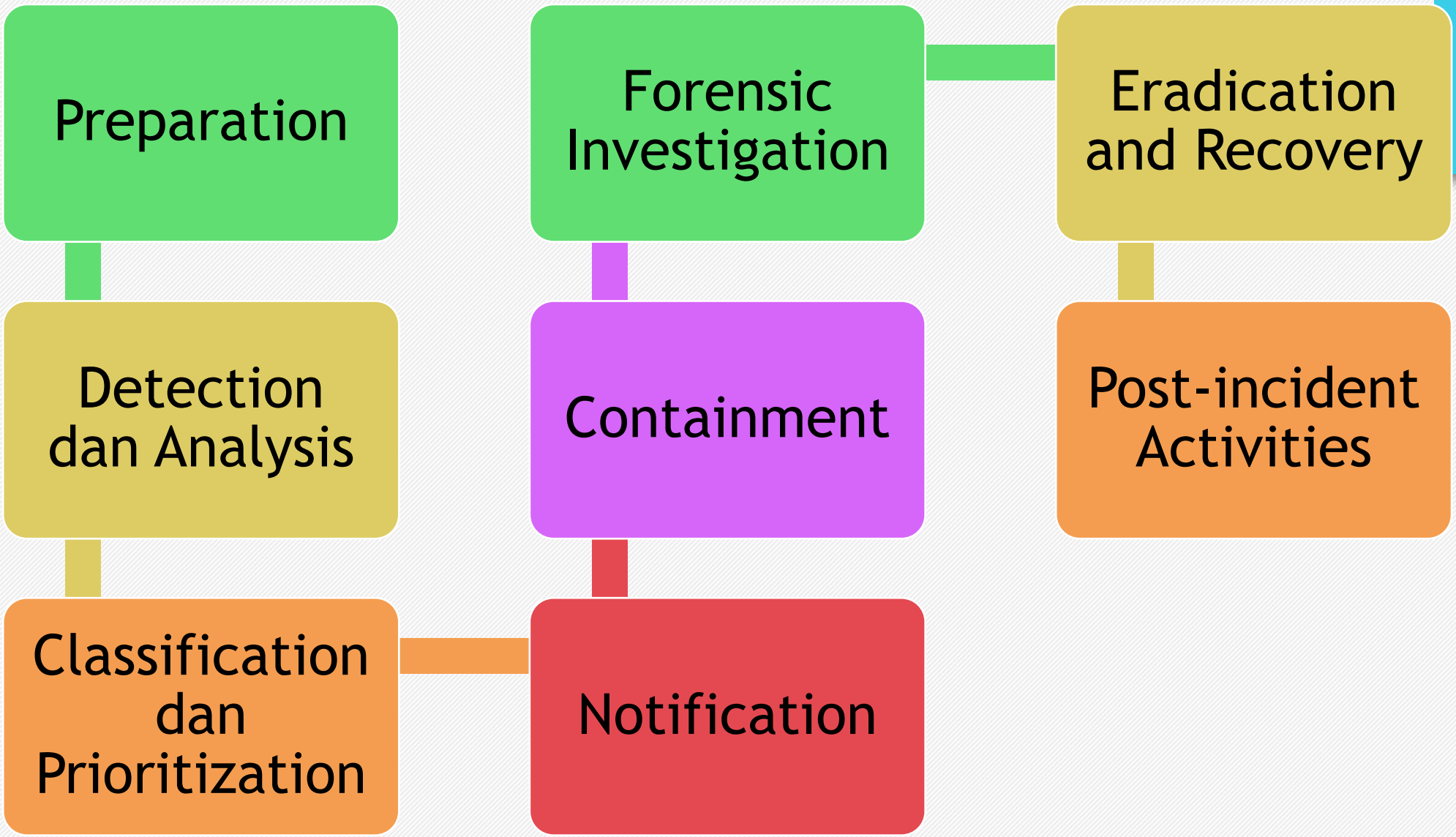
Namun demikian, semua dari kita harus memahami Incident Response Plan yang telah disusun oleh organisasi yang berisi:

- Nama dan kontak informasi dari IRT terdekat/local
- Prosedur eskalasi
- Prosedur pelaporan dan penaganan sebuah security event
- Tindakan lokalisir untuk setiap tipe insiden

First Response Steps by Network Administrator

Hindari Fear, Uncertainty, and Doubt (FUD)	• Jangan Panik, Eskalasi dan Konsultasikan dengan tim forensic
Lakukan Initial Incident Assessment	• Periksa apakah insiden tersebut legit atau False Positive
Komunikasikan Insiden	• Hubungi Kontak terdekat sesuai SOP IRT
Lokalisir Kerusakan	• Disconnect atau biarkan tetap connected ke jaringan
Kendalikan akses terhadap device yang dicurigai	• Amankan perangkat utama dan perangkat lain di sekitarnya, monitor sampai tim IRT datang
Kumpulkan informasi tentang device tersebut	• Kumpulkan informasi perangkat: IP, name, installed app/services, dll
Catat setiap aktivitas	• Catat setiap aktivitas investigasi yang dilakukan: Waktu, saksi
Tahan diri untuk melakukan investigasi lebih jauh	• Tahan diri untuk menginvestigasi terlalu dini, kesalahan dapat merusak bukti di pengadilan
Jangan ubah kondisi/status device	• Biarkan perangkat tetap ON atau tetap OFF, perubahan state-nya dapat menghilangkan bukti yang diperlukan
Disable Proteksi Virus	• Antivirus dapat mengakses/ubah timestamp, dapat menghapus suspected filepada perangkat • Dapat mempersulit investigasi forensik

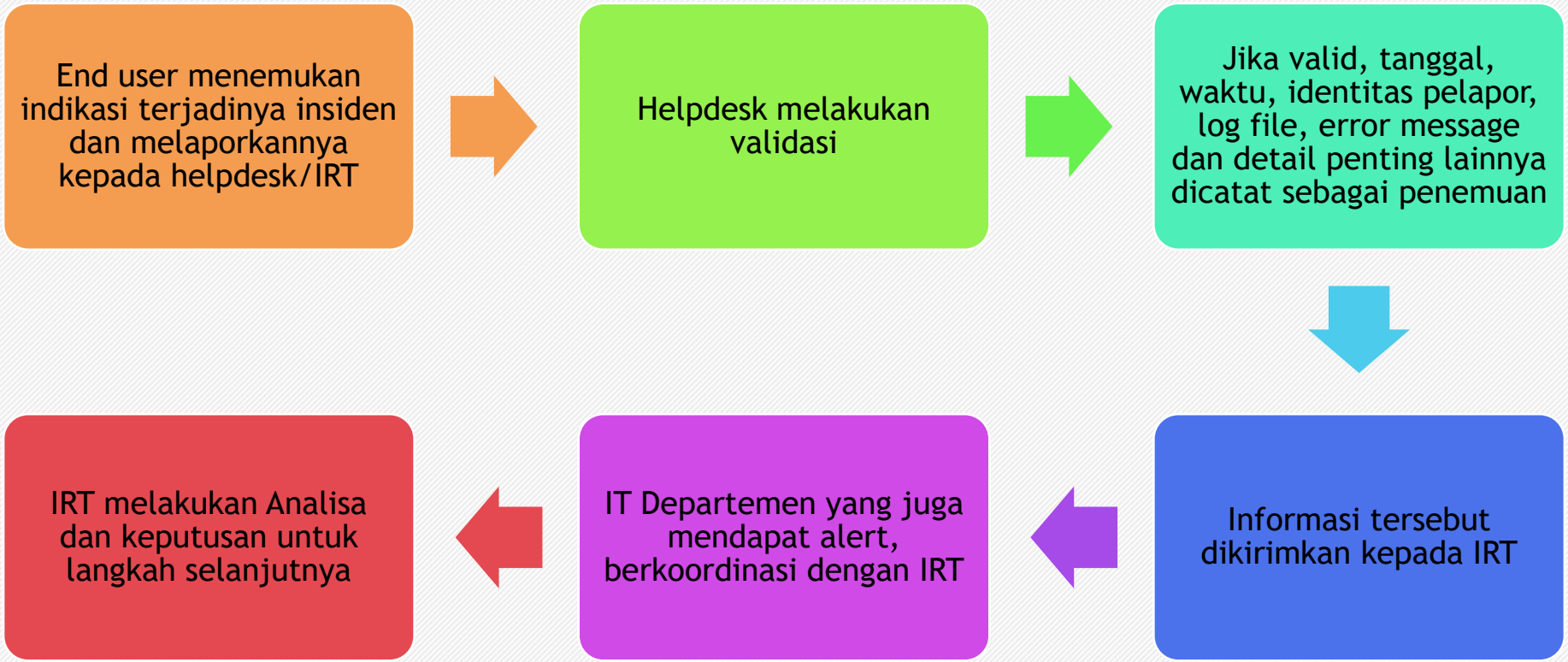
PROSES IH&R


Preparation
Forensic Investigation
Eradication and Recovery
Detection dan Analysis
Containment
Post-incident Activities
Classification dan Prioritization
Notification

PROSES IH&R

1. Preparation for IH&R
   - Diawali dengan pembuatan IRT dan training serta penyiapan tools dan resources
   - Dilanjutkan dengan security and risk assessment kondisi terkini organisasi serta implementasi standar keamanan tertentu

2. Detection and Analysis



PROSES IH&R

3. Classification and Prioritization
   - IRT Manager mengklasifikasikan dan memprioritaskan insiden berdasarkan level high, medium atau low
   - Prioritas ditentukan berdasarkan: tingkat keparahan, target yang terdampak, atau jumlah target yang terdampak
   - Sedangkan klasifikasi bisa ditentukan berdasarkan tipe insiden (serangan eksternal atau internal), legal/regulasi yang terkait
   - Sehingga insiden tidak dihandle berdasarkan First-Come, First-Serve

4. Notification and Planning
   - Komunikasi berperan penting dalam kecepatan penanganan insiden
   - Komunikasi yang baik dibutuhkan karena melibatkan koordinasi antar stakeholder yang terkait dengan insiden
   - Pihak yang perlu di-notify berikutnya adalah Management terkait
   - Management diperlukan dalam memberikan persetujuan tentang rencana penanganan insiden
   - Jika diperlukan, organisasi dapat menghubungi IRT/Tim Forensik eksternal untuk membantu. Namun sebelumnya diperlukan procedure dan perjanjian Kerjasama yang baik untuk menjaga kerahasiaan data

5. Containment
   - Containment adalah Langkah antisipatif untuk meminimalisir perluasan dampak insiden
   - Containment juga berarti menjaga atau mengamankan data supaya data tidak berubah (integrity), sehingga kualitas forensic menjadi sah dan valid

PROSES IH&R

5. Forensic Investigation
   - Investigasi Forensik adalah proses pengumpulan bukti yang terkait dengan insiden baik dari sistem maupun jaringan
   - Tujuan utama dari investigasi adalah menemukan jenis insiden, attacker, waktu kejadian, dan Langkah mitigasi yang diperlukan untuk menghindari insiden berulang
   - Tantangan dari Proses Forensik adalah mengumpulkan data yang melebihi kapasitas storage dan melakukannya dengan menjamin integritas data
   - Tipe bukti yang diperlukan adalah Host-based, Network based dan Other evidence

6. Eradication and Recovery
   - Eradication adalah pemusnahan semua penyebab (root cause) dari insiden
   - Vulnerability Assessment Kembali diperlukan pada fase ini beserta tahapan countermeasure-nya
   - Recovery adalah Langkah mengembalikan data yang hilang baik menggunakan proses forensic maupun data backup

8. Post-Incident Activities
   - IRT melakukan dokumentasi seluruh aktivitas penanganan insiden
   - Biaya dan dampak kerusakan dan recovery insiden dapat menjadi factor Ketika menuntut attacker di pengadilan
   - Setelah dokumentasi dan recovery selesai, review-lah prosesnya